NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE PORT SECURITY GRANT PROGRAM: GOOD ENOUGH, OR CAN IT BE MADE BETTER?

by

Paul D. J. Arnett

June 2016

Thesis Advisor:	Rudy Darken
Second Reader:	Ryan Ellis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the 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 Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE THE PORT SECURITY GRANT PROGRAM: GOOD ENOUGH, OR CAN IT BE MADE BETTER?			**5. FUNDING NUMBERS**
6. AUTHOR(S) Paul D. J. Arnett			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number NPS.2016.0006-IR-EP7-A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

For almost a decade and a half since the terrorist attacks of September 11, 2001, the Port Security Grant Program has provided funding to project proposals for improving the security and resiliency posture of the nation's ports and waterways. The United States has over 360 coastal and inland ports through which over $1.3 trillion in cargo moves annually; a safe, secure, and efficient MTS is critical to national security. The PSGP is intended to enhance port security and resiliency by funding proposals to provide increased risk management, measures to mitigate disruptions and facilitate port recovery, and maritime domain awareness (MDA) capabilities to prevent, respond to, and recover from attacks. The PSGP has matured to include funding for all-hazards threatening the ports—natural, accidental, and intentional. This thesis seeks to evaluate how well the PSGP has met those goals and if it should be improved, reorganized or eliminated.

14. SUBJECT TERMS Port Security Grant Program, Maritime Transportation Security Act, Area Maritime Security Committee			**15. NUMBER OF PAGES** 149
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE PORT SECURITY GRANT PROGRAM: GOOD ENOUGH, OR CAN IT BE MADE BETTER?

Paul D. J. Arnett
Captain, United States Coast Guard
B.A., Salisbury State College, 1985
M.S., St. Joseph's University (Philadelphia), 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2016

Approved by: Dr. Rudy Darken
Thesis Advisor

Dr. Ryan Ellis
Second Reader

Dr. Erik Dahl
Associate Chair of Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For almost a decade and a half since the terrorist attacks of September 11, 2001, the Port Security Grant Program has provided funding to project proposals for improving the security and resiliency posture of the nation's ports and waterways. The United States has over 360 coastal and inland ports through which over $1.3 trillion in cargo moves annually; a safe, secure, and efficient MTS is critical to national security. The PSGP is intended to enhance port security and resiliency by funding proposals to provide increased risk management, measures to mitigate disruptions and facilitate port recovery, and maritime domain awareness (MDA) capabilities to prevent, respond to, and recover from attacks. The PSGP has matured to include funding for all-hazards threatening the ports—natural, accidental, and intentional. This thesis seeks to evaluate how well the PSGP has met those goals and if it should be improved, reorganized or eliminated.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. PROBLEM SPACE 1
- B. RESEARCH QUESTION 12

II. RESEARCH STRUCTURE AND METHODS 15
- A. FOUNDATION DOCTRINE 15
- B. ACADEMIC DISCOURSE 15
- C. OTHER LITERATURE 16
- D. SURVEYS 16
- E. INTERVIEWS 16

III. FOUNDATION DOCTRINE 19
- A. FOUNDATION DOCTRINE 19
  - 1. U.S. Patriot Act and U.S. Homeland Security Act 19
  - 2. Presidential Directive21/PPD-21—Critical Infrastructure and Resilience 21
  - 3. Maritime Transportation Security Act (MTSA) 22
  - 4. U.S. Coast Guard Navigation and Inspection Circulars (NVIC) 26
  - 5. National Response Framework (NRF) and National Incident Management System (NIMS) 29
  - 6. National Strategy for Maritime Security (NSMS) 29
  - 7. National Infrastructure Protection Plan (NIPP) 39
  - 8. Port Security Grant Program (PSGP) Guidance 43
  - 9. Government Accountability Office (GAO) Audits 51
  - 10. Congressional Research Service (CRS) 53
  - 11. Other Federal Reports 55
- B. ACADEMIC, RESEARCH, AND WHITE PAPERS 57
- C. OTHER SOURCES 63
  - 1. Stakeholders Survey 63
  - 2. Stakeholder Interviews 66

IV. ANALYSIS 67
- A. FINDINGS FROM LITERATURE REVIEW 67
- B. FINDINGS FROM SURVEYS 71
- C. FINDINGS FROM INTERVIEWS 80
  - 1. The Coast Guard MS-RAM Program 80

2. PSGP Broadly 80
3. PSGP Specifically' 82
D. REPRESENTATIVE EXAMPLES—FAILURE FROM LACK OF RESILIENCY 87
1. OCIA Analysis of Poe Lock Disruption 87
2. OCIA Analysis: Consequences to Seaport Operations from Malicious Cyber Activity 92
3. Transfer of PSGP HLS Boat 95
E. INTERPRETATION, ANALYSIS, FUSION AND SYNTHESIS OF ALL RELEVANT DATA AND EVIDENCE 98

V. RECOMMENDATIONS 101
A. MAINTAIN THE PSGP AS A DISCRETE GRANT PROGRAM 101
B. IMPROVE TRANSPARENCY OF PROPOSAL REVIEW AND GRANT AWARD PROCESS 101
C. JETTISON THE COOKIE CUTTER 102
1. Allow the Employment of Fiduciary Agents and Consortia as an Option 102
2. Not all Ports are the Same 104
3. Require AMSC's to maintain the PRMP/ BCRTP 106
4. Cost Sharing; Less is More for the Private Sector 107
5. Core Capabilities as PSGP Objectives Must Be Revised 107
6. Re-visit the Risk Equation 109

VI. CONCLUSION 111

LIST OF REFERENCES 115

INITIAL DISTRIBUTION LIST 125

LIST OF FIGURES

Figure 1. Description of MARSEC Levels. Source: 33 CFR §101.105. 24

Figure 2. Elements of Regulations. Source: 33 CFR §103. 26

Figure 3. NSMS Situational Awareness, Prevention and Response, and External Communications. Source: National Strategy for Maritime Security. 31

Figure 4. Core Capabilities of the NPG Mission. Source: NPG Core Capabilities, FEMA.gov (2015). 33

Figure 5. Core Capabilities of the National Preparedness System. Source: National Preparedness System. 34

Figure 6. Maritime Infrastructure Recovery Plan–Plan Relationship Map. Source: National Strategy for Maritime Security: The Maritime Infrastructure Recovery Plan 2006. 35

Figure 7. A Systems View of the MTS Source: National Strategy for Maritime Security–Maritime Transportation System Security Recommendations. 37

Figure 8. Concept Schematic. Source: National Strategy for Maritime Security–Maritime Transportation System Security Recommendations. 38

Figure 9. Statements of the NIPP. Source: DHS, National Infrastructure Protection Plan (2013). 39

Figure 10. Security-Resilience Relationships. Source: NIPP 2013. 41

Figure 11. NIPP Mission Statement and Goals. Source: NIPP 2013, Transportation Sector SSP. 42

Figure 12. Port State Control Grant Process. Source: Notice of Funding Opportunity Fiscal Year 2015 Port Security Grant Program (PSGP). 45

Figure 13. Initial PSGP Ports and Eligible Expenditures. Source: FY 2003 UASI Port Security Grant Program NOFO. 46

Figure 14. Source: PSGP FY 2005, 36 Target Capabilities List Critical Capabilities. 48

Figure 15. Survey Page 1. 64

Figure 16. Survey Page 2. 65

Figure 17. Survey Page 3. 66

Figure 18. Survey Results. 74

Figure 19. Survey Results. 75

Figure 20. Survey Results. 76

Figure 21. Survey Results. 77

Figure 22. Screenshot from Google Earth accessed 06 March 2016. 88

Figure 23. Screenshot from University of Texas at Austin, Cockrell School of Engineering, *UT Austin Researchers Spoof Superyacht at Sea***,** Monday, Jul 29, 2013, http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea. 94

Figure 24. FEMA letter regarding disposition of Homeland Security SAFE Boat. 97

LIST OF TABLES

Table 1. FY2008 through FY2015 PSGP Funding Guidelines.....50

Table 2. Survey Response Summary for the Remaining Questions.....78

Table 3. All Survey Responses. 79

Table 4. Initial Allocations of Port Security Grants. Source: The Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program.....105

Table 5. Allocated Grant Fund by Tiered Port. Source: Fiscal Year 2007 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit. 106

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAPA	American Association of Port Authorities
ACP	Area Contingency Plan
AIS	Automated Identification System
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
ARRA	American Recovery and Reinvestment Act
BCRTP	Business Continuity/Resumption of Trade Plans
CAP	Center for American Progress
CBP	U.S. Customs and Border Patrol
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CI	Critical Infrastructure
CIKR	Critical Infrastructure / Key Resources
COTP	Captain of the Port (USCG)
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FMSC	Federal Maritime Security Commander
FSP	Facility Security Plan
GAO	Government Accountability Office
GPD	Grants Programs Directorate (FEMA)
IED	Improvised Explosive Device
ISPS	International Ship and Port Security Code
MARAD	US Maritime Administration (DOT)
MDA	Maritime Domain Awareness
MSAC	Maritime Security Advisory Committees
MSRAM	Maritime Security Risk Analysis Model
MSRT	Maritime System Response Team
MSST	Maritime Safety and Security Teams
MTS	Marine Transportation System

MTSA	Maritime Transportation Security Act
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
ODP	Office for Domestic Preparedness (DHS)
PANAMAX	Refers to ships whose dimensions are the maximum capable of transiting the Panama Canal
PRMP	Port-Wide Risk Mitigation Plans
PSGP	Port Security Grant Program
SHSP	State Homeland Security Program
SLGCP	Office of State and Local Government Coordination and Preparedness (DHS)
SOLAS	Safety of Life at Sea Code
SSP	Sector Specific Plans (of the NIPP)
TEU	Twenty-foot Equivalent Unit (a 20'x8'x8' standard intermodal shipping container)
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Credential
UASI	Urban Area Security Initiative
USCG	U.S. Coast Guard
WMD	Weapons of Mass

EXECUTIVE SUMMARY

For almost a decade and a half since the terrorist attacks of September 11, 2001, the Port Security Grant Program has provided funding to projects with the intention of improving the security posture of the nation's ports and waterways. The United States has over 360 coastal and inland ports through which over $1.3 trillion in cargo moves annually; a safe, secure, and efficient MTS is critical to national security.[1] "[T]he PSGP is [intended] to provide funding to the nation's highest risk port areas to support increased port-wide risk management; to enhance domain awareness; to train and exercise; to expand port recovery and resiliency capabilities; and to further capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices and other nonconventional weapons."[2] This inquiry evaluated how well the PSGP has met those goals and determine if it can be improved, reorganized or has fulfilled its role and should be eliminated.

Methodology

The primary focus of this study is a consideration of policy options analysis for the Port Security Grant Program (PSGP). In this effort, a combination of literature review, interviews, and surveys methodologies was utilized.

At the outset, a thorough review of relevant literature was conducted. The topical content of the literature review included:

[1]Josh Peters, "Overview of the United States Coast Guard's Cyber Strategy and the MTS" (presentation, Ninth Coast Guard District, Cleveland, OH, March 29, 2016).

[2]Government Accountability Office, "Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measurements Should be Strengthened," GAO-12-47, Month Day, 2012, http://www.gao.gov/products/GAO-12-47 (accessed January 6, 2016), 1–2.

- *Foundation Doctrine*—the laws, regulations, policies, and guidelines that define the national expectations for port security;
- *Academic Discourse*—thesis, dissertations, peer-reviewed journals, white papers, research papers, studies, and similar documents;
- *Other Literature*—Media, blogs, non-peer-reviewed journals and publications, and mass media.

The survey was a short series of questions consisting of a mix of demographic questions, yes/no responses, multiple choice options, and seven point Likert Scale assessments. The respondents were subject matter experts and stakeholders of the Port Security Grant Program.

Interviews were conducted with national level program managers and smaller subset of stakeholders. The questions were free-form, specific to the respondent's experience with the PSGP, with some input from the survey results to initiate the conversation.

Analysis

There is a tremendous amount of literature on the topic of grants in general and the Port Security Grant Program specifically. The spectrum of references included official government reports, academic papers, white papers, industry analysis, statistical reports, and more. Unfortunately, the response to the survey was small, although apparent patterns are discernible. While not statistically supportable, the responses were useful in guiding the conversations during the interviews, which were exceptionally insightful.

Recommendations

The Maritime Transportation System (MTS) is a system-of-systems construct. It is an emergence outcome from the continually evolving interaction between commercial and regulatory actors. The foundation policies, from the Presidential Directives to the National Infrastructure Protection Plan recognize

the complex network that sustains the MTS across multiple Critical Infrastructure (CI) Sectors.

By being armed with that knowledge and understanding, the best programmatic approach to the Port Security Grant Program (PSGP) should be one that seeks to promote systems solutions for investing in improved port security and resiliency. However, the history of the PSGP has been a moving target, ultimately focusing on individual port entities and stakeholders rather than port-wide systems solutions. To counter that imbalance between national policy and program strategy, the following recommendations are suggested:

- *Maintain the PSGP as a Discrete Grant Program.* Periodically, factions of both the Legislative and Executive Branches of the Federal Government have suggested eliminating the PSGP as a specific, discrete grant program, and instead rolling it into a homeland security block grant. Ports would then have to compete against all other jurisdictions and communities for grant funding. The ports are national borders through which over 90% of our international trade takes place. They represent a last opportunity to prevent a terrorist attack using the maritime nexus. A natural disruptive event would also have grave cascading economic consequences, particularly for companies that depend on just-in-time processes. Disruption to the MTS would weaken all other systems and make interior jurisdictions more vulnerable.

- *Improve Transparency of Proposal Review and Grant Award Process.* The PSGP is almost universally criticized by the port stakeholders competing for grants through their Area Maritime Security Committees (AMSC) for failing to keep applicants and AMSCs informed. No feedback is provided to applicants whose proposals fail to win grants. There is no feedback provided to the AMSCs as to why the national program managers modify their proposed port priorities. Transparent communications between the program managers and stakeholder communities must be improved.

- *Jettison the Cookie Cutter.* The standard guidelines for submitting PSGP proposals throughout its existence have been a “one-size-fits-all” model, treating all ports as a homogeneous construct. The PSGP has, with few exceptions, targeted grants to single entities rather than seeking to award port-wide proposals. While the foundation doctrine speaks of the MTS complexity as a system of systems, the PSGP addresses port security and resiliency from a

reductionist point of view. The PSGP has to recognize that each port is different and system-wide solutions, including the allowance for consortia, is a valuable option to addressing port security and resiliency gaps and should be accepted as grant applicants. The former port tier/group system was a valuable tool for prioritizing grant awards and should be restored to the PSGP.

- *Fully Employ Port-wide Risk Management Plans (PRMP).* PRMPs provide value-added identification of port-wide security and resiliency gaps and a roadmap for developing a gap closure strategy. PRMPs provide for measurable goals and supportable investment justifications (IJ). They also look at solving problems from the MTS level, rather than the individual entity level. PRMPs should be required resources for all AMSC, kept up to date, and referenced in IJs.

- *Keep Cost Sharing at 25% for All Stakeholders.* The Cost Share contribution has been a moving target across PSGP iterations. At times, the private sector share has been 50% while the public sector remained at 25%. A flat rate for all stakeholders encourages greater participation and should be made a permanent feature of the PSGP.

- *PSGP Core Capabilities Objectives Must Be Revised.* The objectives for PSGP funding has remained essentially unchanged over the course of the program's life. Some of the core capabilities have been demoted, others resolved, and others still simply stale. It is time to revise the objectives for port security grants, with a focus on enhancing port resiliency and port-wide systemic solutions.

- Replace references to the Risk Equations as

***R**isk = **V**ulnerability X **T**hreat X **C**onsequence*

with

R= f[(V)(T)(C)]

That is, Risk is a Function of the relationships between Vulnerability, Threat, and Consequence.

Conclusion

The PSGP has not evolved sufficiently over the course of its existence. There have been occasions where programmatic changes were implemented,

only to be eliminated in future iterations. The Fiduciary Agent, allowance for consortia to compete for grant funds, the grouping of ports into different tiers by consequent risk, flat 25% cost share for all applicants, and the requirement for Port-wide Risk Management Plans are prime examples. The tendency for the PSGP is to approach port security and resiliency as a cookie-cutter, the one-size-fits-all program fails to acknowledge the variation between ports and that the MTS is a system of systems. The insistence that grants be awarded only to individual entities further exacerbates the disconnection between national level policy and the PSGP guidance.

The PSGP can be a tremendously valuable vehicle for improving the overall security and resiliency of the nation's MTS, but it has to be flexible enough to respond to the unique conditions of each port system competing for grant funding. It also must have a means for measuring the success of awarded proposals regarding risk bought down. The PRMP provides that metric. PRMPs must be a requisite part of all AMSCs and referenced in grant proposals. The program managers must evaluate the efficacy of awarded proposals at filling the security and resiliency gaps they seek to close. The PRMP provides the scale for that measurement.

The Port Security Grant Program is a valuable tool for improving port security and resiliency. But, indeed, it can be made better.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis could not have been done without a great deal of help. First, I extend my deepest appreciation to those stakeholders in the Port Security Grant Program. You were wonderfully open and candid with your insights and experiences. I hope that this work provides a step forward in advancing port security and resiliency.

My family felt the daily sacrifice of my secluding myself away for many hours. It took its toll and took away precious time together. Your love and support were the critical infrastructures that kept me moving forward.

My Coast Guard supervisors were equally committed to my success, recognizing the value of continuing education and lifelong learning. Thank you for the opportunity and support.

CHDS Cohort 1405/06. I believe we are unique amongst those cohorts that preceded us and set a high bar for those that follow. Our commitment to each other for support, direction, friendship and survival were very much like a family. It is my honor to know you and to have been able to go on this ride with you.

Of course, the faculty and staff at Naval Postgraduate School, Center for Homeland Defense and Security, were our navigators on this incredible journey. Thank you for the gift of this experience and the tools I will take with me. In particular, I want to thank Dr. Rudy Darken, my thesis advisor, and Dr. Ryan Ellis, my second reader, who kept me on course.

Thank you, all. *Semper Paratus*, and may you always have fair winds and following seas.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The vulnerability of our critical infrastructure was made painfully apparent in the aftermath of the September 11, 2001, attack on the United States. Congress established the Port Security Grant Program (PSGP) in the wake of that realization. The security and resiliency of the nation's ports and waterways—its Maritime Transportation System (MTS)—is essential to our national economy and is complementary to our land borders and airports as controlled boundaries for the movement of persons and materials into and out of the United States' jurisdiction. The United States has over 360 coastal and inland ports through which over $1.3 trillion in cargo moves annually; a safe, secure, and efficient MTS is critical to national security.[1] The Government Accountability Office (GAO) noted that "[T]he PSGP is [intended] to provide funding to the nation's highest risk port areas to support increased port-wide risk management; to enhance domain awareness; to train and exercise; to expand port recovery and resiliency capabilities; and to further capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices and other nonconventional weapons."[2] This inquiry seeks to evaluate how well the PSGP has met those goals and determine if it can be improved, reorganized or has fulfilled its role and should be eliminated.

A. PROBLEM SPACE

The Nation clearly recognized the criticality of the national infrastructure to both our physical and economic security in the wake of the 9–11 attacks. A series of Presidential Directives have been subsequently issued that directs the federal government to undertake efforts to enhance the security and resiliency of

[1] Josh Peters, "Overview of the United States Coast Guard's Cyber Strategy and the MTS" (presentation, Ninth Coast Guard District, Cleveland, OH, March 29, 2016).

[2] Government Accountability Office, "Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measurements Should be Strengthened," *GAO-12-47,* Month Day, 2012, http://www.gao.gov/products/GAO-12-47 (accessed January 6, 2016), 1-2.

our critical infrastructure; the latest iteration is PPD-21, Critical Infrastructure Security and Resilience issued February 12, 2013. PPD-21 mandates that the federal government work across the Departments and Agencies, in partnership with State, Local, Territorial, and Tribal (SLTT) jurisdictions, and in collaboration with the private sector. It recognizes the necessity for public-private coordination given that the vast majority of critical infrastructure resides in the private sector. PDD-21 further directs measures be taken to effectively "strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation's safety, prosperity, and well-being."[3]

The reference to "systems" is significant. The United States' defines its ports and waterways as components of the Marine Transportation System (MTS). It is not merely a set if independent entities situated along the waterways that interface with ships for transportation, it is a system of components: businesses, communities, governmental agencies, military facilities, jurisdictions, intermodal links, international borders, labor, and natural resources. Much of American industry is located along the nation's navigable waterways to take advantage of the availability of transportation, process water, co-location with major population centers and intermodal transportation hubs. For these same reasons, most U.S. power generation—which uses the conversion of water into steam to make electricity—is located on waterways. As pointed out by Steven Flynn, director of the Center for Resilience Studies and co-director of the George J. Kostas Research Institute for Homeland Security at Northeastern University,

> responding to today's challenges, the threats of terrorism and natural disasters requires the broad engagement of civil society. … Sustaining the United States' global leadership and economic competitiveness ultimately depends on bolstering the resilience of its society. Periodically, things will go badly wrong. The United

[3] Presidential Policy Directive / PPD-21 (Washington, DC: The White House, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 9, 2016).

> States must be prepared to minimize the consequences of those eventualities and bounce back quickly.[4]

Following the terrorist attacks of September 11, 2001, the United States was confronted with the profound need to assess its security posture across all modes of transportation rapidly. Congress responded by establishing a series of grant programs, each targeting various modes of, or nexuses with, the transportation sector. Of those grant programs, one specifically addressed the gaping vulnerability presented by our expansive coastline and relatively unsecured ports and waterways system.

> The Port Security Grant Program (PSGP) provides grant funding to port areas for the protection of critical port infrastructure from terrorism. PSGP funds are primarily intended to assist ports in enhancing maritime domain awareness, enhancing risk management capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices (IEDs), weapons of mass destruction (WMDs) and other non-conventional weapons, as well as training and exercises and Transportation Worker Identification Credential (TWIC) Implementation.[5]

It is important to note that the nation's ports are our primary economic gateway, by far outstripping all other avenues of trade. The Maritime Administration stated "[i]n 2011, U.S. waterborne trade (foreign and domestic) amounted to over 2.1 billion metric tons, up slightly from the year before. Foreign trade accounted for 62.5% of the total, up from 59.8% five years earlier."[6]

Over 99% of the U.S. overseas trade by weight—65% by value—is moved through the nation's deep-water ports--accounting for over $3.15 trillion[7] of

---

[4] Stephen E. Flynn, "America the Resilient Defying Terrorism and Mitigating Natural Disasters," *Foreign Affairs* (2008), http://www.nyu.edu/intercep/lapietra/Flynn_AmericatheResilient.pdf, accessed January 9, 2016.

[5] Department of Homeland Security, "American Recovery and Reinvestment Act of 2009, Port Security Grant Program Guidance and Application Kit," May 2009, p.3 .http://www.fema.gov/pdf/government/grant/arra/fy09_arra_psgp_guidance.pdf (accessed January 7, 2016).

[6] Maritime Administration, "2011 U.S. Water Transportation Statistical Snapshot," November 2013, p. 3, http://www.marad.dot.gov/wp-content/uploads/pdf/US_Water_Transportation_Statistical_snapshot.pdf (accessed October 2, 2014).

[7] American Association of Port Authorities, *"U.S. Public Port Facts,"*, last modified 2013, http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032.

revenue. However, before 9/11, U.S. port security was principally focused on preventing and deterring criminal activity through access controls and law enforcement intelligence for crew and cargo vetting, in particular for smuggling of contraband cargoes. The September 2001 terror attacks changed that. As practiced, pre-9/11 port security represented a gaping vulnerability in our nation's security posture. Attackers could exploit ports in two ways: a direct attack on the port itself intended to cripple the economy where over 90% of all U.S. trade was transacted or as a portal for smuggling persons and materiel into the mainland. If the standard was to prevent criminal activity, activities in support of terrorist plots might go undetected. The first significant law that focused on maritime and port security was the Marine Transportation Security Act (MTSA), key provisions of which are:

- Vulnerability assessments of facilities and vessels;
- National, area, facility and vessel security plans, and facility and vessel incident response plans;
- Transportation security cards—known as Transportation Worker Identification Credential (TWIC);
- Port Security Grant Program (PSGP);
- Coast Guard managed programs of:
- Regionally sited Maritime Safety and Security Teams (MSST);
- Maritime Security Advisory Committees (MSAC);
- Security Assessments of Foreign Ports (primarily fulfilled under the International Ship and Port Security (ISPS) Code, an amendment to the Safety of Life at Sea (SOLAS) Code);
- Vessel Automated Identification System (AIS);
- Enhancement of Cargo and Intermodal Shipping Security.[8]

The Coast Guard has been responsible for the security of the ports and waterways of the United States during times of war since the enactment of the

[8] Joseph F. Bouchard, Ph.D., "New Strategies to Protect America: Safer Ports for a More Secure Economy" (Center for American Progress, Washington, DC, 2005), 6.

Espionage Act of 1917. After World War II, the Magnuson Act of 1950 assigned the Coast Guard an ongoing mission to safeguard U.S. ports, harbors, vessels, and waterfront facilities from accidents, sabotage, or other subversive acts.[9]

The Homeland Security Act of 2002 reinvigorated the Coast Guard's historical national defense mission by emphasizing Ports, Waterways and Coastal Security (PWCS) as the Service's primary homeland security mission.[10]

The September 11, 2001, terrorist attacks amplified the significance of the Coast Guard's historic mission to protect the homeland. In response to the attacks, the Maritime Transportation Security Act (MTSA) was passed. Coast Guard Sector Commanders are the designated Federal Maritime Security Coordinators (FMSC) in the MTSA. The Coast Guard through the FMSC is the lead agency responsible for coordinating and managing national maritime security and response.[11]

In response, the Coast Guard undertook its largest reorganization since its assimilation of the predecessor agencies that resulted in the creation of the U.S. Coast Guard. The new organization model revolves around supporting the dual operational missions of Prevention and Response.

The Coast Guard PWCS mission comprises attainment of Maritime Domain Awareness (MDA), protection and restoration of the Maritime Transportation System (MTS); law enforcement and anti-terrorism measures; and response and recovery to man-made and natural disruptions to the MTS. The 2005 terrorist attacks on the London transit system, the 2008 Mumbai terror attacks from the sea, and Hurricanes KATRINA and RITA underscore the critical importance of preparation and planning for the PWCS mission to protect, respond to, and recover from events impacting the U.S. critical infrastructure and

---

9 *"U.S. Coast Guard, Missions, Maritime Security,"* last Modified September 5, 2014, http://www.uscg.mil/top/missions/MaritimeSecurity.asp (accessed November 02, 2014).

10 *"U.S. Coast Guard, Ports, Waterways & Coastal Security (PWCS),"* last modified January 12, 2016, http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

11 *"U.S. Coast Guard, Missions, Maritime Security,"* last Modified September 5, 2014, http://www.uscg.mil/top/missions/MaritimeSecurity.asp. (accessed November 02, 2014).

key resources (CIKR). To fulfill the PWCS mission, the Coast Guard manages a "systematic, maritime governance model for PWCS employs a triad consisting of domain awareness, maritime security regimes, and maritime security and response operations carried out in a unified effort by international, governmental, and private stakeholders."[12]

The Port Security Grant Program (PSGP), through the MTSA-established Area Maritime Security Committees (AMSC), guided by the Federal Maritime Security Coordinator (FMSC), is a component of the PWCS process of engaging port stakeholders to enhance the security posture of U.S. maritime domain.

The purpose of the PSGP is to facilitate the hardening and building of resiliency into the nation's port infrastructure, to protect and mitigate from damage caused by natural and man-made events, while also facilitating the rapid resumption of business, continuity of operations, and integrity of the marine transportation system (MTS).

The Port Security Grant Program is part of the national strategy to "strengthen America's critical infrastructure."[13] The ultimate effort seeks to "reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure."[14]

> The United States has approximately 360 commercial sea and river ports. While no two ports in the United States are exactly alike, many share certain characteristics that make them vulnerable to terrorist attacks: they are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks designed to move cargo and commerce as quickly as possible. They contain not only terminals

---

12 *"U.S. Coast Guard, Ports, Waterways & Coastal Security (PWCS),"* last modified January 12, 2016, http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

13 Department of Homeland Security, *"Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit,"* 2005, 1, www.fema.gov/pdf/government/grant/psgp/fy05_psgp_guidance.pdf,(accessed January 7, 2016).

14 *Presidential Directive / PPD-21*—Critical Infrastructure Security and Resilience (Washington, DC: The White House, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed October 11, 2015).

> where goods bound for import or export are unloaded or loaded onto vessels, but also other facilities critical to the nation's economy, such as refineries, factories, and power plants.[15]

This same vulnerability to terrorist attack makes ports, and the entire MTS, vulnerable to any disruptive impact, natural or man-made, intentional or accidental.

The PSGP targeted constituencies are state, local, tribal, and private port region stakeholders. State and local law enforcement and emergency management agencies that serve in the nation's ports and waterways system, often with co-jurisdiction and overlapping areas of operation with the U.S. Coast Guard,[16] and sometimes each other, are eligible to compete for Port Security Grants. Private sector stakeholders, who own and manage over 90% of the port infrastructure, are also eligible to compete for PSGP funding. The greatest distinction between the public and private sector competition is the percentage of matching funds[17] required for a given proposal: private entities generally must match 50% of the proposal while public sector applicants must match 25%.,[18][19] The combined public and private sector constituencies bounded within a U.S. Coast Guard Sector area of operation, defines the eligible membership of the regional Area Maritime Security Committee (AMSC).

The PSGP has often been criticized for apparent inefficiencies, waste, mismanagement, ever-changing precepts and guidelines, and ever-changing administrators. These criticisms have led some within Congress and the Administration to call for eliminating the dedicated Port Security Grant Program,

---

[15] Government Accountability Office, "Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measurements Should be Strengthened," *GAO-12-47,* 2012, 5, http://www.gao.gov/products/GAO-12-47 (accessed January 6, 2016).

[16] The Coast Guard cannot compete for PSGP funds, nor can it directly benefit from any grant proposals.

[17] Requirements for grant seekers to contribute proportional matching contributions to PSGP project proposals varies from year to year, and may be eliminated completely during any given grant cycle.

[18] GAO-12-47, 30.

[19] In 2016 the cost share became a flat 25% for public and private sector applicants.

and instead incorporate port grants into a single homeland security grant program or merge into the existing Urban Area Security Initiative (UASI) grants program. Department of Homeland Security (DHS) Secretary Chertoff addressed the problem with the critiques during a 2007 press conference on the overarching Infrastructure Protection Grants Program. His concerns were that the UASI program covered a wide range of grants, whereas the Port Security Grant Program was specific to the ports. In this way, the ports would have expressly allocated funds to address security at our ports of entry, before the threats to national security via that vector entered the United States. In that same press conference, he addressed the stories of waste and inefficiencies:

> Predictably, we had a rash of stories, which I still read occasionally, about communities that spent money on leather jackets or gym equipment or things of that sort. And so to move away from that kind of willy-nilly approach, we have put in place–and I think this year [FY07] really affects the maturation of that process–a risk driven allocation of eligibility but a capabilities drive determination of what the actual grants are, so that we really make sure that the money goes for the kinds of things I think the public expects, things like situational awareness, cameras to show you where the risks are, or the tools you need in order to respond if there is an attack upon a ship in a port …. And I think the combination of risk driven eligibility but a disciplined approach to making sure the grants are spent on the appropriate risk-reduction efforts delivers exactly what the American public expects.[20]

He further went on to state that those examples were in the early days of the post-9/11 grant programs and that "the problem … was not that there was fraud; it's that the requirements were defined so broadly and so generally that anything that could be tied to homeland security, in theory, was eligible." [21] A review of the early PSGP application guidelines confirms his assessment.

---

[20] U.S. Department of Homeland Security, "*Remarks by Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2007 Infrastructure Protection Grants Program,"* January 09, 2007, 4-5.

[21] Department of Homeland Security, "*Remarks by Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2007 Infrastructure Protection Grants Program,"* January 09, 2007, 7.

At its launching, the PSGP was one of many homeland security grant programs that public and private constituencies saw as opportunities to offset their costs in complying with new laws promoting enhanced security, such as with the Maritime Transportation Security Act (MTSA).[22] They were established to help offset costs, but there was an expectation that the grant funds be applied toward applications that would also reduce risk.

> The program is attempting to reconcile the goals of the Maritime Transportation Security Act of 2002 (MTSA), the competitive grant program mandated by Congress, and risk-based direction of grant monies. MTSA is a nationwide security mandate that widely affects the maritime industry. The program is faced with the competing pressures of offsetting MTSA related costs while making competitive and risk-based grant decisions to protect the nation's most critical ports and port facilities.[23]

With 40 deep-water ports[24] capable of at least handling PANAMAX[25] ships dotting more than 82,000[26] miles of coastline, the amount of area to protect from infiltration is staggering. In 2010, the U.S. imported over 17.6 million TEUs[27] and exported 11.2 million TEUs, first place in imports and second place in exports worldwide.[28]

---

[22] "MTSA II," a regulatory update to the MTSA that will harmonize the MTSA regulations with new laws since MTSA was passed, including the SAFE Port Act and ISPS Code, is currently in the Notice of Proposed Rule Making (NPRM) process.

[23] Department of Homeland Security, Office of the Inspector General. *Review of the Port Security Grant Program (OIG-05-10).* (Washington, DC: 2005), 4.

[24] AAPA number of Panamax capable ports. It is important to note that port classifications under the PSGP can, and often do, change.

[25] PANAMAX (ships whose dimensions are the maximum capable of transiting the Panama Canal).

[26] Wikipedia contributors, "List of countries by length of coastline," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=List_of_countries_by_length_of_coastline&oldid=692497936 (accessed January 10, 2016).

[27] TEU = twenty foot equivalent units, meaning the equivalent of volume of containers if all were uniformly shipped in 20' by 8' by 8' standard freight containers.

[28] World Shipping Council, *"Trade Statistics,"* last modified 2014, http://www.worldshipping.org/about-the-industry/global-trade/trade-statistics.

The Center for American Progress (CAP)[29] took aim at the Port Security Grant Program in a 2006 white paper titled "*New Strategies to Protect America: Safer Ports for a More Secure Economy*." Despite its obvious political animus towards the George W. Bush administration, the white paper authored by Joseph F. Bouchard, Ph.D., articulated many common frustrations with the PSGP at the time, and made some recommendations for overcoming those shortcomings for a viable, solid port security program. In it, the CAP proposed four strategies for improving the PSGP that would assure more secure U.S. ports and waterways and the economy dependent upon them. The primary focus advocated utilization of a risk-based methodology that melded enhanced security to buy down potential consequences while enhancing preparedness, resilience, and continuity of business.

Specifically, those points were:

- Revise Coast Guard maritime facility regulations to focus on the threat and consequence portion of the Risk Equation, rather than to focus on hardening facilities to reduce vulnerability. The Risk Equation is

$$\boldsymbol{R}isk = \boldsymbol{V}ulnerability \times \boldsymbol{T}hreat \times \boldsymbol{C}onsequence$$

If necessary, amend the MTSA to do so:

- Emphasize marine transportation system (MTS) risk mitigation, preparedness and continuity of operations to deny terrorists a strategic target and reduce the economic impact of attack;

[29] The CAP is a "think tank" headquartered in Washington, DC, and formerly lead by John Podesta. Mr. Podesta was Chief of Staff for President Clinton, and a counselor on President Obama's White House Staff.

- Keep the PSGP, but allow for more program flexibility in the proposals and increase the annual appropriated funding to a minimum of $500M; and
- Establish a National Port Security Trust Fund from a percentage of customs revenue collected.[30]

Certainly, given that the ports are the "front line" of defense, from which the remainder of the country benefits, the ports deserve a targeted grant program dedicated to assisting building MTS resiliency, enhancing security, and establishing collaborative planning and response preparedness practices and relationships. By ensuring the security and resiliency of the ports, the rest of the county benefits by:

- Preventing the threat from entering the country by sea in the first place; and
- Protecting the economic lifeblood of the nation--the primary avenues of trade.

Additionally, all of the variables in the Risk Equation should be on the table for consideration, as well as the validity of the Risk Equation itself, rather than only focusing on one or two aspects over any other. Buying down any of the variables will reduce the Risk potential.

The Port Security Grant Program is part of the national strategy to "strengthen America's critical infrastructure."[31] The ultimate effort seeks to "reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure."[32]

- The PSGP is an outcome of the 9/11 attacks, designed to provide guidance and targeted, risk-based funding grants to improve the security and resiliency of the United States' ports as critical infrastructure.

---

[30] Joseph F. Bouchard, Ph.D., "New Strategies to Protect America: Safer Ports for a More Secure Economy" (Center for American Progress, Washington, DC, 2005), 2.

[31] Department of Homeland Security, *"Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit,"* 2005, 1, www.fema.gov/pdf/government/grant/psgp/fy05_psgp_guidance.pdf,(accessed January 7, 2016).

[32] *Presidential Directive / PPD-21*—Critical Infrastructure Security and Resilience.

- Entering assumptions for this study include:
- The nation's ports are critical to national security, including sovereignty, public safety, and economic vitality.
- The PSGP provides essential support to improving the status quo of port security, but there is room for improvement
- The nation's ports are a potential target of terrorist attack, an avenue for exploiting access into the United States, and any disruption to port operations—whether from a natural disaster or man-made event—may pose grave safety and economic impact.
- Known and potential limitations in this study include:
- Time constraint; the available time to conduct research and analysis sufficient to develop a viable thesis is, by necessity, constraining;
- Limited Target Population; due to time constraint, only a representative sample of port stakeholders will able to participate.

B. RESEARCH QUESTION

The Port Security Grant Program is part of the national strategy to "strengthen America's critical infrastructure."[33] The ultimate effort seeks to "reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure."[34]

There are still many questions outstanding, such as:

- The subject of this research is the Port Security Grant Program (PSGP). The research assessed whether and to what degree the policy has been effective in attaining its stated goal of improving port security and resiliency, or alternative policy options would be more effective.
- What does "risk-based" mean in the context of the maritime transportation system (MTS) as critical infrastructure?

---

[33] DHS, *"Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit,"*

[34] *Presidential Directive / PPD-21*—Critical Infrastructure Security and Resilience (Washington, DC: The White House, 2013).

- How well does the Port Security Grant Program align with the national policies and strategies it is intended to support7? What does success or money well spent look like?
- How can the Port Security Grant Program (PSGP) be designed to maximize national defense, critical infrastructure protection (CIP), and port/MTS resiliency?
- Is the R = (V)(T)(C) an appropriate or realistic model for assessing "risk" for the purpose of allocating financial resources for mitigation measures to protect the MTS?

THIS PAGE INTENTIONALLY LEFT BLANK

II. RESEARCH STRUCTURE AND METHODS

The primary focus of this study is a consideration of policy options analysis for the Port Security Grant Program (PSGP). In this effort, a combination of literature review, interview, and surveys methodologies was utilized.

A thorough review of relevant literature was conducted. The topical content of the literature review included:

- *Foundation Doctrine*—the laws, regulations, policies, and guidelines that define the national expectations for port security;
- *Academic Discourse*—thesis, dissertations, peer-reviewed journals, white papers, research papers, studies, and similar documents.
- *Other Literature*—Media, blogs, non-peer-reviewed journals/ publications, mass media.

A. FOUNDATION DOCTRINE

Original doctrine was reviewed to establish initial port security policy and expectations for the Port Security Grant Program. The study progressed through the PSGP evolution, and the overarching laws, policies, and regulations that shaped the PSGP's focus over time, and ultimately, defined the current theater of operations for the PSGP. This first level of focus in the literature review is called *Foundation Doctrine*.

B. ACADEMIC DISCOURSE

The next targeted literary review focused on the academic literature dealing with port security, critical infrastructure protection (CIP), the PSGP, and some consideration of frameworks for evaluating port security and resiliency analysis, and discourse on risk and resiliency as policy determinants. This section, called Academic Discourse, will consisted of reviewing academic and research literature, professional and peer-reviewed journals, and white papers. This section injected analytic frameworks, critiques, and opportunities for consideration from observers outside of the vested stakeholders.

C. OTHER LITERATURE

The final category of literature considered is the catch-all, Other Literature. This material is from outside of the peer-reviewed or governmental publications associations. These materials include the mass media, online blogs, non-peer-reviewed journals and publications, other Internet sources (such as YouTube, Wikipedia, and news aggregators).

D. SURVEYS

A short survey with select subject matter experts (SME) was conducted. The survey consisted of 20 questions that are a mix of demographic questions, yes/no answers, multiple choice options, and seven point Likert Scale questions.

E. INTERVIEWS

Interviews conducted with select subject matter experts (SME). The SMEs are representative of the Port Security Grant Program stakeholder network. These include the U.S. Coast Guard, Federal Emergency Management Administration (FEMA), and public and private members of Area Maritime Security Committees (AMSC) for selected ports. This last group includes maritime facility owner/operators, vessel owner/operators, shipping agencies, other Federal, State, and local public safety and regulatory agencies, port authorities, maritime exchanges, and homeland security experts.

An analysis of the combined results of the literature review, survey, and interviews with subject matter experts was performed to determine to what degree the PSGP has succeeded in meeting its stated goal of improving port security and the resiliency of the MTS. The analysis sought to define more clearly such terms as “risk-based assessment,” “resiliency,” and “critical infrastructure.” Also considered is the appropriateness of Risk Equation [R = (V)(T)(C)] as a model for effectively determining the best course of actions for improving port security. Variations of, and alternatives to, the risk model are considered that

may be more appropriate or may supplement the Risk Equation for enhancing the PSGP process.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FOUNDATION DOCTRINE

The data and evidence analyzed in this research are from topical literature, respondent surveys, and direct interviews of essential subject matter experts with the first-hand experience of stakeholders with the Port Security Grant Program, both program administrators, and port grant applicants. Content categories parse the Literature Review.

A. FOUNDATION DOCTRINE

The importance of protecting essential infrastructure elements became immediately apparent during the response to the September 11, 2001, al-Qaida airliner attacks. The downing of the World Trade Center (WTC) twin towers not only destroyed the lives of those that perished and the ones that loved them, but it also unleashed a cascade of massive impacts across the Nation's infrastructure. Telecommunications was knocked out in lower Manhattan and cellular service over a much larger area. All United States ports were shut down and vessels ordered to remain either offshore, at berth, or anchorage. All non-military aviation was grounded. The bridges and tunnels into and out of New York were closed. New York's public safety system was overwhelmed, as well as suffering its horrific loss of responding heroes.

1. U.S. Patriot Act and U.S. Homeland Security Act

The first Act of Congress in response to the horrific attacks was passage and subsequent signing into law of the controversial U.S. Patriot Act of 2001. The term "critical infrastructure" was defined in the Patriot Act as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or

any combination of those matters."[35] Protection of infrastructure information and cyber-security solidified as an essential security concern in the Patriot Act.[36]

It is interesting to note that the vulnerability of our "critical infrastructure" was identified as a key security concern before the September 11, 2001 attacks. President Clinton issued PDD/NSC-63, Critical Infrastructure Protection on May 22, 1998. In it, the Whitehouse recognized the evolving nature of what has become recognized as critical infrastructure vulnerability. The opening section presages what would become a greater national concern after the attacks:

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.
>
> Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."[37]

---

[35] U.S. Patriot Act of 2001, 42 U.S.C. 5195(e) (2001).

[36] Homeland Security Act of 2002, 6 U.S.C.§101 (2002).

[37] *Presidential Decision Directive/NSC-63* (Washington, DC: The White House, 1998), http://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed January 9, 2016), 1.

Later, the Homeland Security Act of 2002 further defined ‘‘key resources’’ as those “publicly or privately controlled resources essential to the minimal operations of the economy and government.”[38] The President promulgated *Homeland Security Presidential Directive 7 (*HSPD-7*): Critical Infrastructure Identification, Prioritization, and Protection* on December 17, 2003, to further amplify the importance of critical infrastructure (CI) and key resources (KR). HSPD-7 made the first connections between the importance of protecting U.S. CIKR and adding to the discussion of prevention, protection, and security, the concept of resiliency.

The most recent update to the National Infrastructure Protection Plan (NIPP 2013) recognizes “security” and “resiliency” as complementary aspects of a thorough homeland security plan. The Executive Summary stated “[o]ur national well-being relies upon secure and resilient critical infrastructure—those assets, systems, and networks that underpin American society. To achieve this security and resilience, critical infrastructure partners must collectively identify priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment.”[39] From the start, CIP has been understood to be the joint responsibility of both the public and private sectors; the private sector owns and manages the vast majority of CIKR, but the responsibility for establishing a national security strategy resides with the government.

Together the public and private sector stakeholders will collaboratively protect, defend, and make more resilient our CIKR.

2. Presidential Directive21/PPD-21—Critical Infrastructure and Resilience

On February 12, 2013, President Obama issued Presidential Policy Directive 21–Critical Infrastructure Security and Resilience (PPD 21). PPD-21

[38] Homeland Security Act of 2002, 6 U.S.C. §101 (2002).

[39] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)* 2013, 1.

has further refined the importance of protecting our CIKR: "The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure–including assets, networks, and systems–that are vital to public confidence and the Nation's safety, prosperity, and well-being."[40] At this point, the policy makers realize the interconnectedness and complexity of the United States' critical infrastructure—that it is a distributed network system, in fact, greater than that—it is a system of systems. The concepts of *security* and *resiliency* are now linked; resiliency is part of the security calculus for protecting CIKR. The policy-makers appreciation for our ubiquitous dependence on information technologies has also matured, with *cyber-security* an essential component of any security strategy.[41]

> Critical infrastructures are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[42]

A new concept is being brought forward; *unity of effort*. Unity of effort speaks to the cross-sector collaboration that is essential to any effective CIKR security strategy. No one agency, company, or interest has sole control over all aspects of any segment of the CIKR. Such is the nature of the system of systems.

3. Maritime Transportation Security Act (MTSA)

Making the U.S. CIKR more secure and resilient is a daunting and expensive undertaking. The Maritime Transportation Security Act (MTSA) sought, in part, to help offset the cost while guiding the development of strategic enhancements to port security through the Port Security Grant Program (PSGP).

---

[40] Presidential Directive / PPD-21—Critical Infrastructure Security and Resilience.

[41] Ibid.

[42] Presidential Directive / PPD-21—Critical Infrastructure Security and Resilience.

The MTSA was another powerful and far-reaching law passed in the wake of the September 11, 2001, attacks, but focused on securing the maritime vector. Critical elements of the MTSA related to the PSGP and port security include:

- That threat and vulnerability assessments be conducted for U.S. ports and domestic and foreign commercial vessels (over 100 gross register tons), and concomitant security plans and security response plans for each;
- Establishment of a National Maritime Security Plan and Advisory Committee and Area Maritime Transportation Security Plans and Committees;
- Transportation Worker Identification Credential (TWIC) for controlling access to marine facilities and vessels;
- Coast Guard rapid response force elements capable of quick deployment to areas of impact or sites requiring short term enhanced security called Maritime Safety and Security Teams (MSST);
- The Port Security Grant Program (PSGP), and more maritime-specific programs and enhancements.[43]

In 2006, the MTSA was amended and certain provisions clarified and enhanced with the passage of the Security and Accountability for Every (SAFE) Port Act. The SAFE Port Act sought to add "risk-based funding through a dedicated Port Security Grant Program to harden U.S. ports against terrorist attacks and enhance capabilities to respond to attacks and resume operations."[44] Other SAFE Port Act enhancements include requirements to establish joint federal, state, local and stakeholder command centers; procedures for restoration of trade and the maritime transportation system following a transportation security incident, deployment of nuclear and radiation detection capabilities at the Nation's ports, and programs and processes for preventing threats from overseas.

---

[43] Department of Homeland Security, *Maritime Transportation Security Act of 2002 Press Kit*: *Protecting America's Ports*, July 2003, 1-12.

[44] House Committee on Homeland Security, *The SAFE Port Act Fact Sheet*, March 2006, 1.

Title 33 Code of Federal Regulations, Subchapter H promulgates the MTSA implementing regulations. Subchapter H also attempts to align MTSA requirements with the International Code for the Security of Ships and of Port Facilities (ISPS Code)—an amendment to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) as SOLAS Chapter XI-2, to which the United States is signatory. The MTSA regulations define terms for enforcement, including the Coast Guard's Maritime Security Levels (MARSEC), which require holders of vessel and facility security plans to activate the additional security measures identified in their plans upon elevation of the MARSEC level. The MARSEC levels are shown in Figure 1.[45]

LEVEL	DESCRIPTION
MARSEC 1	The level for which minimum appropriate protective security measures shall be maintained at all times.
MARSEC 2	The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.
MARSEC 3	The level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

Figure 1. Description of MARSEC Levels. Source: 33 CFR §101.105.

The Commandant of the Coast Guard sets the MARSEC Level based on the threat environment, although the local Captain of the Port may raise the level based on locally available information at COTP discretion. However, only the

[45] Electronic Code of Federal Regulations, "Title 33: Navigation and Navigable Waters, Part 101 Maritime Security: General, Subpart C-General, Records Retention, and Enforcement, 101.105 Definitions," http://www.ecfr.gov/cgi-bin/text-idx?SID=06484778d56042f2ad2adb178235c8df&mc=true&node=se33.1.101_1105&rgn=div8 (accessed January 07, 2016).

Commandant may lower the MARSEC Level once elevated.[46] Coast Guard enforcement of 33 CFR Subchapter H, the Maritime Transportation Security Act, is under the authorities of 33 CFR Parts 6, 160 and 165.

Regulations defining the COTP designation as Federal Maritime Security Coordinator (FMSC) and the attendant authorities are codified in 33 CFR §103—Maritime Security: Area Maritime Security. This same section defines the Area Maritime Security Committee (AMSC), the requirements for conducting the MTSA-required Area Maritime Security Assessments (AMSA), and the development of Area Maritime Security Plans (AMSP). Elements of each include in part are described in Figure 2.

[46] Electronic Code of Federal Regulations, "Title 33: Navigation and Navigable Waters, Part 101 Maritime Security: General, Subpart B-Maritime Security (MARSEC) Levels,

101.200 MARSEC Levels," http://www.ecfr.gov/cgi-bin/text-idx?SID=06484778d56042f2ad2adb178235c8df&mc=true&node=se33.1.101_1200&rgn=div8 (accessed January 07, 2016).

CONCEPT	DESCRIPTION
FMSC	The COTP for a given Coast Guard Sector will be the FMSC. The FMSC is responsible for establishing and overseeing an AMSC, appointment of its membership, and direct development of the AMSP.
AMSC	The AMSC will operate under a written charter per 33 CFR §103.300, comprised of federal, territorial, state, Tribal, and local public safety, law enforcement, and crisis management agencies, the maritime industry, other port stakeholders and have clear background investigations. Terms of service will be no greater than five years. AMSC responsibilities include identification of CIKR, identification of port risks (i.e., threats, vulnerabilities, and consequences), determination of mitigation measures and strategies, assist with the development of the AMSP, help communicate MARSEC level changes and dissemination of port security information.
AMSA	The AMSC will ensure completion of a risk-based AMSA per 33 CFR §103.310, §101.510 and §103.405.
AMSP	The AMSP should address MARSEC changes, defensive measures to prevent contraband security smuggling, unauthorized access to secure locations, transportation security incident (TSI) reporting procedures, CIKR protection, response to alerts procedures, suspicious activity report handling, and more. Also addressed in the AMSP are plan exercise and recordkeeping provisions.

Figure 2. Elements of Regulations. Source: 33 CFR §103.

4. U.S. Coast Guard Navigation and Inspection Circulars (NVIC)

The publication of regulations always generates anxiety, confusion, and often additional cost for the regulated communities. The rapid-fire pace of new security-related regulations in response to the 2001 attacks exacerbated those challenges. To mitigate the concern and expedite compliance, the Coast Guard issued a series of Navigation and Vessel Inspection Circulars (NVIC) that clarify

compliance with the new laws and their regulations. The prime series of MTSA implementation NVICs are:

- NVIC 04–02: Security for passenger vessels and passenger terminals.
- NVIC 09–02: Guidelines for the development of area maritime security committees and area maritime security plans required for U.S. Ports.
- NVIC 10–02: Security guidelines for vessels.
- NVIC 11–02: Recommended security guidelines for facilities.
- NVIC 03–03: Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities.
- NIVC 04–03: Guidance for verification of vessel security plans on domestic vessels by the regulations mandated by the Maritime Transportation Security Act (MTSA) Regulations and International Ship & Port Facility Security (ISPS) code.
- NVIC 05–03: Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 for Outer Continental Shelf Facilities.
- NVIC 10–04: Guidelines for Handling of Sensitive Security Information (SSI), parts 1 and 2.
- NVIC 12–04: Maritime security compliance and enforcement for the U.S./Canadian boundary and coastal waters.
- NVIC 02–05: International Port Security (ISP) Program.
- NVIC 03–07: Guidance for the implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector.
- NVIC 01–13: Inspection and Certification of Vessels Under the Maritime Security Program (MSP)

Of essential interest here is NVIC 09–02, *Guidelines for the development of area maritime security committees and area maritime security plans required for U.S. Ports*. It is a 218-page tome that addresses each of the new initiatives mandated in the combined MTSA and SAFE Port Act specific to the newly

created Area Maritime Security Committees and their chartered responsibilities, as well as providing unifying definitions of terms for performing the AMS Assessments and developing the AMSPs for their geographic region. The overarching goal of the AMSC is the institutionalization of "[c]ollaborative planning, coordination, open lines of communication, strong working relationships, and unity of effort are essential to provide an effective systems approach to preventing, detecting, responding, and recovering from terrorist threats to the MTS."[47] NVIC 09–02 goes into great detail on:

- What skill sets the AMSC needs;
- The proper handling of sensitive security information (SSI);
- Protected Critical Infrastructure Information (PCII);
- Conducting the AMS Assessments and use of the Coast Guard's Maritime Security Risk Analysis Model (MSRAM);
- The concepts of "Maritime Common Operating Picture (MCOP)"; and
- AMS Exercises (including the Area Maritime Security Training and Exercise Program or AMSTEP).[48]

In particular, it is the AMSCs that provide input and "technical support for evaluation of port security grant proposals in support of AMSPs."[49] In most cases, it is AMSC members that are competing for the PSGP funds. NVIC 09–02 provides the first deeper explanation of the Coast Guard's MSRAM tool in describing how to build a viable AMSP:

> The first step in developing and maintaining the AMSP is completing or revalidating an Area Maritime Security Assessment. The most current and valid port and facility data should be entered into the Maritime Security Risk Analysis Model (MSRAM), which then uses the data to calculate relative risk based on the Coast Guard Risk-Based Decision Making (RBDM) methodology (using a

[47] U.S. Coast Guard, "NVIC 09-02: Guidelines for development of area maritime security committees and area maritime security plans required for U.S. Ports.," 2002, 3.

[48] U.S. Coast Guard, "NVIC 09-02, 3-4.

[49] Ibid., 4.

"Threat X Vulnerability X Consequence" algorithm). Each of the components of the formula is broken down into multiple benchmarks with weighted numerical values. The MSRAM analysis results in a scenario-based Risk Index Number (RIN) that can be used to formulate the ranking of assets within a port or jurisdiction, and support the development or updating of AMS Assessments as required by 33 CFR § 101.510, § 103.400, § 103.410, and § 103.510.[50]

5. National Response Framework (NRF) and National Incident Management System (NIMS)

Area Maritime Security Plans are designed around the MARSEC tiered system. As MARSEC level moves up from Level 1 to 2, and ultimately 3, the security posture for the vessel or facility covered by the AMSP is elevated to match the potential for a transportation security incident (TSI). It is important to note that the AMSP is a component of the National Response Framework (NRF)[51] and must be consistent with the NRF, and harmonized with the National Incident Management System (NIMS).

6. National Strategy for Maritime Security (NSMS)

A slew of national strategies and plans were published after September 11, 2001, and focused on providing guidance and structure to our national preparedness posture. The emphasis was on hardening, making more resilient, and pre-identifying courses of action, processes, and procedures for preventing deterring, mitigating, responding to, and recovering from natural or man-made disasters. The intention is to provide a clear framework for establishing national security strategies and practices. Those that bear most directly on port security are:[52]

---

[50] Ibid., Appdx2-1.

[51] The National Response Framework (NRF) replaced the National Response Plan (NRP) as the national level contingency model for responding to All-Hazards events utilizing the National Incident Management System (NIMS).

[52] *National Security Presidential Directive–NSPD-41/Homeland Security Presidential Directive HSPD-13*— Maritime Security Policy (Washington, DC: The White House, 2004), http://fas.or/irp/offdocs/nspd/nspd41.pdf (accessed January 30, 2016).

- National Strategy for Maritime Security
- National Plan to Achieve Domain Awareness
- Global Maritime Intelligence Integration Plan
- Maritime Operational Threat Response Plan
- International Outreach and Coordination Strategy
- Maritime Infrastructure Recovery Plan
- Maritime Transportation System Security Plan
- Maritime Commerce Security Plan
- Domestic Outreach Plan

The National Strategy for Maritime Security (NSMS) depends upon the execution of eight Plans/Strategies that in concert fulfill the directive promulgated by National Security Presidential Directive 41 (NSPD-41)/Homeland Security Presidential Directive 13 (HSPD-13): National Maritime Security Policy. Together, they form the National Strategy for Maritime Security. The constituent Plans/Strategies of the NSMS, while all interrelate with one another to accomplish the whole of national maritime security, can be grouped by three task focus areas: Situational Awareness, Prevention and Response, and External Communications, illustrated in Figure 3 from the NSMS. The goal of the NSMS is to be alert for potential, thwart, respond to, and if all else fails, to rapidly recover from a Transportation Security Incident (TSI).[53]

- Situational Awareness: The Plans/Strategies that the comprise the Situational Awareness area are the Global Maritime Intelligence Integration Plan, National Plan to Achieve Maritime Domain Awareness, and the Maritime Operational Threat Response Plan (MOTR).[54]

[53] "*Transportation security incident (TSI)* means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area," 33 CFR §101.105.

[54] The Maritime Operational Threat Response Plan's (MOTR) contents are classified and can only be alluded to in broad generalities in this thesis.

- External Communications: The two Plans/Strategies that most directly concern external communications are the International Outreach Strategy to Enhance Maritime Security, and the Domestic Outreach Plan.

- Prevention and Response: The final Plans/Strategies grouping whose focus is on prevention and response are the Maritime Transportation Systems Security Plan, the Maritime Commerce Security Plan, and the Maritime Infrastructure Recovery Plan.

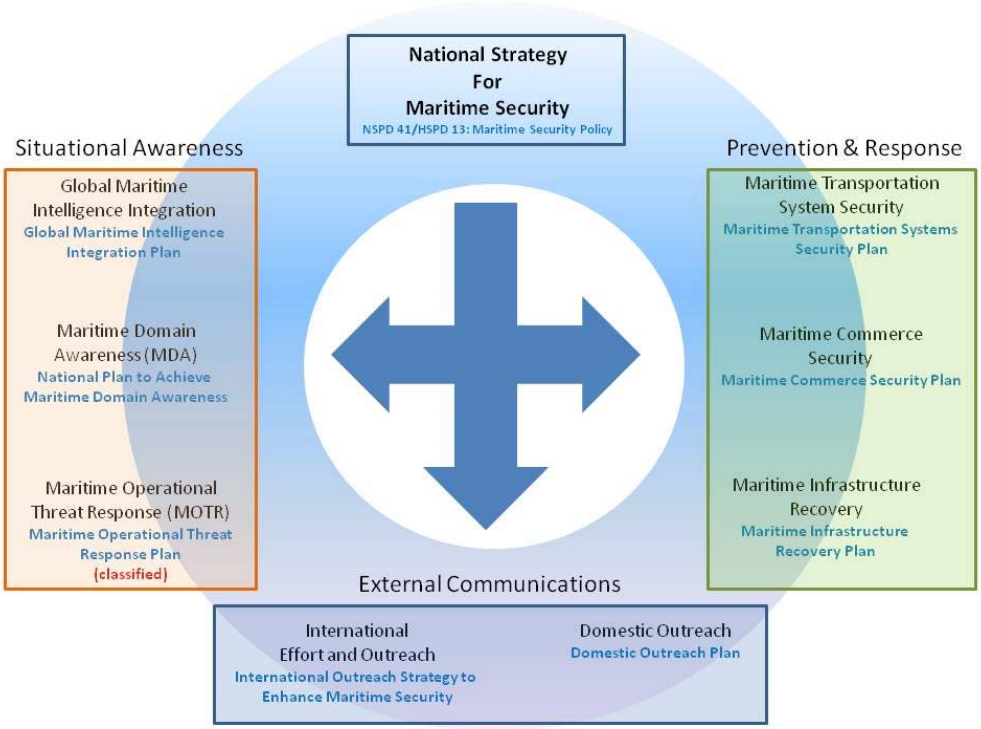


Figure 3. NSMS Situational Awareness, Prevention and Response, and External Communications. Source: National Strategy for Maritime Security.

The National Strategy for Maritime Security (NSMS) aligns with—Homeland Security Presidential Directive 5 (HSPD-5): Management of Domestic Incidents; HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection; Presidential Policy Directive 8 (PPD-8): National Preparedness; and PPD-21: Critical Infrastructure Security and Resilience. The NSMS is part of a constellation of systems, strategies, and plans that provide a framework for the

preparedness continuum of [*planning], "prevention, protection, mitigation, response, and recovery"*[55] to "incidents of national significance"[56] in fulfilling the National Preparedness Goal. Complementary and associated with the NSMS are the National Infrastructure Protection Plan (NIPP) and the components of the National Preparedness Goal (NPG):[57]

- National Preparedness System
- National Incident Management System
- National Planning Framework
- National Prevention Framework
- National Mitigation Framework
- National Response Framework
- National Disaster Recovery Framework

These components enable fulfillment of the thirty-two NPG core capabilities, grouped into five mission areas—many core capabilities fall within multiple mission areas, whereas some support only one. Each mission area—Planning, Prevention, Mitigation, Response, and Disaster Recovery—has its own National Framework (see above).

---

[55] Federal Emergency Management Agency. "FEMA Information Sheet: National Preparedness Goal, Second Edition," FEMA.gov, 1, http://www.fema.gov/national-preparedness-goal (accessed December 10, 2015).

[56] NOTE: When the National Response Plan was superseded by the National Framework, the term "incident of national significance" was eliminated. DHS, "What's New in the National Response Framework," DHS.gov, 2, http://www.fema.gov/pdf/emergency/nrf/whatsnew.pdf, January 22, 2008 (accessed December 10, 2015).

[57] Presidential Policy Directive / PPD-8—National Preparedness (Washington, DC: The White House, 2011), https://www.dhs.gov/presidential-policy-directive-8-national-preparedness (accessed October 11, 2015).

The core capabilities of the NPG mission areas are highlighted in Figure 4.

Core Capability	Mission	Core Capability	Mission
Planning	All	Operational Coordination	All
Public Information & Warning	All	Forensics & Attribution	Prevention
Intelligence & Info Sharing	Prevention Protection	Interdiction & Disruption	Prevention Protection
Screening, Search & Detection	Prevention Protection	Access Control & Identity Verification	Protection
Cyber-security	Protection	Physical Protective Measures	Protection
Risk Mgmt for Protection Programs & Activities	Protection	Supply Chain Integrity & Security	Protection
Community Resilience	Mitigation	Long-Term Vulnerability Reduction	Mitigation
Risk & Disaster Resilience Assessment	Mitigation	Threats & Hazards Identification	Mitigation
Critical Transportation	Response	Environmental Response/Health & Safety	Response
Fatality Management Services	Response	Fire Management & Suppression	Response
Infrastructure Systems	Response Recovery	Logistics & Supply Chain Mgmt	Response
Mass Care Services	Response	Mass Search & Rescue Operations	Response
On-Scene Security, Protection, & Law Enforcement	Response	Operational Communications	Response
Public Health, Healthcare, & Emergency Medical Services	Response	Situational Assessment	Response
Economic Recovery	Recovery	Health & Social Services	Recovery
Housing	Recovery	Natural & Cultural Resources	Recovery

Figure 4. Core Capabilities of the NPG Mission. Source: NPG Core Capabilities, FEMA.gov (2015).

Figure 5 further frames the core capabilities of the National Preparedness System with the mission targets.

<table>
<tr><th>Prevention</th><th>Protection</th><th>Mitigation</th><th>Response</th><th>Recovery</th></tr>
<tr><td colspan="5">Planning</td></tr>
<tr><td colspan="5">Public Information and Warning</td></tr>
<tr><td colspan="5">Operational Coordination</td></tr>
<tr><td colspan="2">Intelligence and Information Sharing</td><td rowspan="5">Community Resilience
Long-term Vulnerability Reduction
Risk and Disaster Resilience Assessment
Threats and Hazards Identification</td><td colspan="2">Infrastructure Systems</td></tr>
<tr><td colspan="2">Interdiction and Disruption</td><td rowspan="4">Critical Transportation
Environmental Response/Health and Safety
Fatality Management Services
Fire Management and Suppression
Logistics and Supply Chain Management
Mass Care Services
Mass Search and Rescue Operations
On-scene Security, Protection, and Law Enforcement
Operational Communications
Public Health, Healthcare, and Emergency Medical Services
Situational Assessment</td><td rowspan="4">Economic Recovery
Health and Social Services
Housing
Natural and Cultural Resources</td></tr>
<tr><td colspan="2">Screening, Search, and Detection</td></tr>
<tr><td rowspan="2">Forensics and Attribution</td><td rowspan="2">Access Control and Identity Verification
Cybersecurity
Physical Protective Measures
Risk Management for Protection Programs and Activities
Supply Chain Integrity and Security</td></tr>
<tr></tr>
</table>

Figure 5. Core Capabilities of the National Preparedness System. Source: National Preparedness System.

The National Strategy for Maritime Security (NSMS) plans are part of the National Preparedness System (NPS) National Response Framework (NRF) and required to be compliant with the National Incident Management System (NIMS). Therefore, all plans must fully utilize the Incident Command System (ICS) structures and align with the National Infrastructure Protection Plan (NIPP). Figure 6 is a plan map that details the interrelationships between the linked plans, strategies, and frameworks that unify the National Strategy for Maritime Security within the National Preparedness System. From the NPS and legislated by the Maritime Transportation Security Act (MTSA), the Area Maritime Security

Committees (AMSC) are mandated. The AMSCs conduct the Area Maritime Security Assessments that the Area Maritime Security Plans address. The MTSA also mandates the development of Vessel Security Plans (VSP) and Facility Security Plans (FSP). Each step is a building block for national security, reinforced one by the other. Figure 6 illustrates the relationships between local and national plan under the National Response Plan (since revised and renamed the National Response Framework).

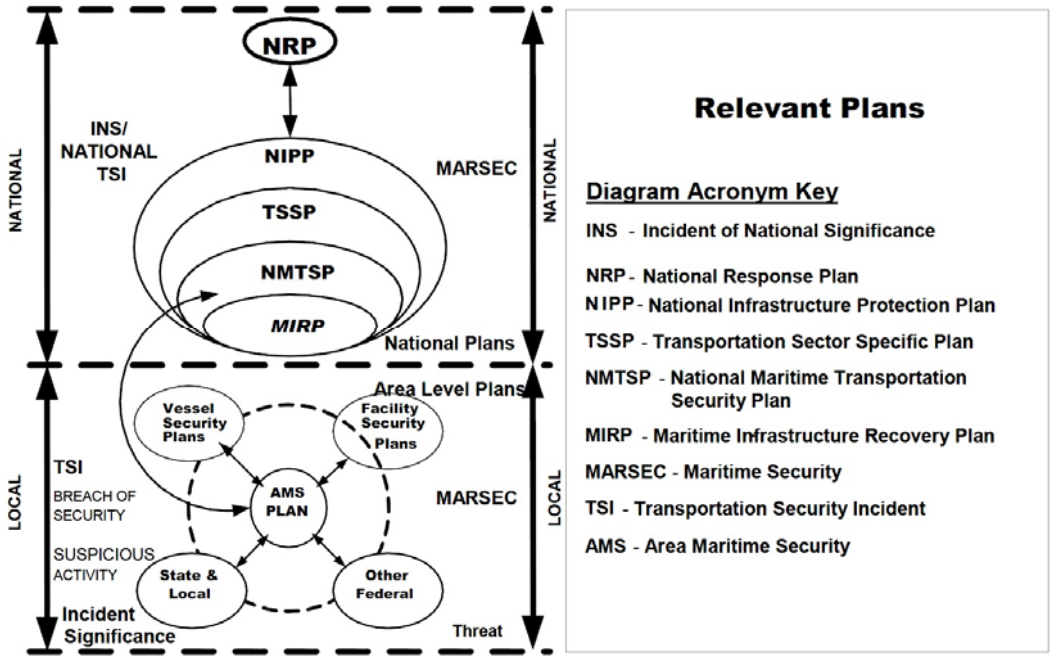


Figure 6. Maritime Infrastructure Recovery Plan–Plan Relationship Map. Source: National Strategy for Maritime Security: The Maritime Infrastructure Recovery Plan 2006.

The NSMS Maritime Transportation System Security Recommendations (MTSSR) establishes a "systems-oriented security regime built upon layers of protection and defense," acknowledging the complexity of the MTS as a system-of-systems.[58] The systems within the MTS noted by the MTSSR are:

[58] Department of Homeland Security. "National Strategy for Maritime Security–Maritime Transportation System Security Recommendations," 3, https://www.dhs.gov/xlibrary/assets/HSPD_MTSSPlan.pdf. (accessed January 30, 2016).

- Component Security—measures to protect the port's physical components, including vessels, vehicles, cargo, terminals, facilities, and other physical port infrastructure.
- Interface Security—measures to make secure intermodal interfaces.
- Information Security—measures to protect data systems and information technologies to include cyber security.
- Network Security—measures to assure the security of the MTS as a whole.[59]

VISION FOR MARITIME TRANSPORTATION SYSTEM SECURITY

A systems-oriented security regime built upon layers of protection and defense in-depth that effectively mitigates critical system security risks, while preserving the functionality and efficiency of the MTS. Understanding the most effective security risk management strategies involves cooperation and participation of both domestic and international stakeholders acting at strategic points in the system, the U.S. seeks to improve security through a cooperative and cohesive effort involving all stakeholders.[60]

The maritime transportation system as a system of systems is graphically displayed in Figure 7.

[59] Ibid., 2.

[60] Ibid., 3.

Figure 7. A Systems View of the MTS[61] Source: National Strategy for Maritime Security–Maritime Transportation System Security Recommendations.

The MTSSR proposes eight strategic recommendations. These include recognition that all stakeholders—public and private sectors—must coalesce to develop holistic strategies to improve the security and resiliency of the MTS. Many of the recommendations are resolved while others remain constantly relevant. The MTSSR recommends application of the following:

(1) Risk management approach,

(2) Protection of critical data and security information,

(3) Concurrent enforcement of national and international security regulations—MTSA and ISPS,

[61] DHS, "National Strategy for Maritime Security–Maritime Transportation System Security Recommendations," C-1.

(4) actively engaging stakeholders for collaborative and coordinated efforts to reduce security risks,

(5) deployment of port access credentials—Transportation Workers' Identity Card (TWIC),

(6) audit existing safety frameworks for opportunities to gain security synergies,

(7) promote development and deployment of port security technologies, and finally,

(8) ensure proper maritime security training of port and maritime personnel.[62]

Figure 8 is the Concept Schematic for the Maritime Transportation System Security Plans Architecture.

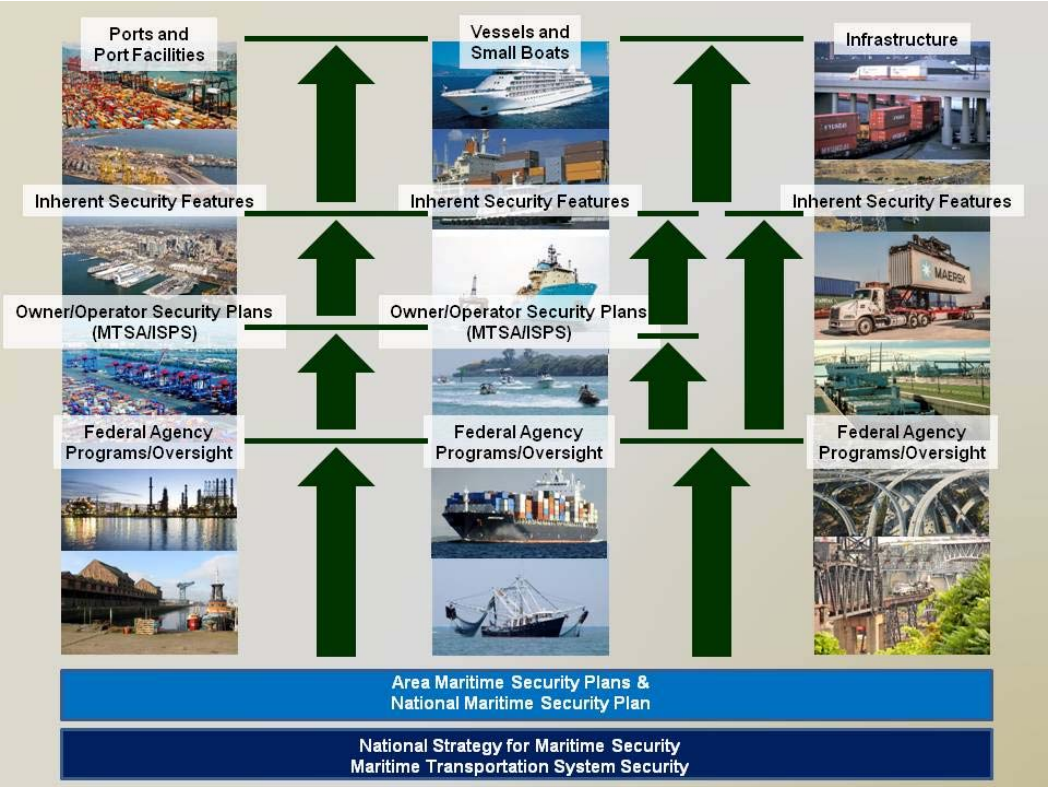


Figure 8. Concept Schematic. Source: National Strategy for Maritime Security–Maritime Transportation System Security Recommendations.

[62] DHS, "National Strategy for Maritime Security–Maritime Transportation System Security Recommendations," 4-13.

7. National Infrastructure Protection Plan (NIPP)

The 2013 edition of the National Infrastructure Protection Plan (NIPP), titled Partnering for Critical Infrastructure Security and Resilience, brings upfront in the CIKR protection equation the importance of building resiliency into the planning process. The concept of resiliency is also fundamental to the Vision, Mission, and Goal statements of the NIPP 2013[63] in Figure 9.

Vision	A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.
Mission	Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.
Goals	Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities; Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments; Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advanced planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services; Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and Promote learning and adaptation during and after exercises and incidents.

Figure 9. Statements of the NIPP. Source: DHS, National Infrastructure Protection Plan (2013).

[63] Department of Homeland Security. "National Infrastructure Protection Plan 2013," 5, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf. (accessed January 30, 2016).

The NIPP 2013 refers to PPD-21 for the definition of resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions … [it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[64] Good intelligence and analysis of risk are essential to being able to identify resiliency building measures. Resilient infrastructure must be not only robust but also flexible enough to adapt to events. Planning efforts that address mitigation, response and recovery strategies are all inputs to building resiliency into infrastructure.[65]

Resiliency is viewed as part of the security continuum, from protective measures to defend against disruptive impact, to the diffusing of vulnerability to be more resilient and recover more quickly from an impactful event. Figure 10 from the NIPP 2013 illustrates this relationship between protection and resiliency on the security continuum.[66]

---

[64] Presidential Directive / PPD-21–Critical Infrastructure Security and Resilience.

[65] DHS, "National Infrastructure Protection Plan 2013," 7.

[66] DHS, "National Infrastructure Protection Plan 2013," 19.

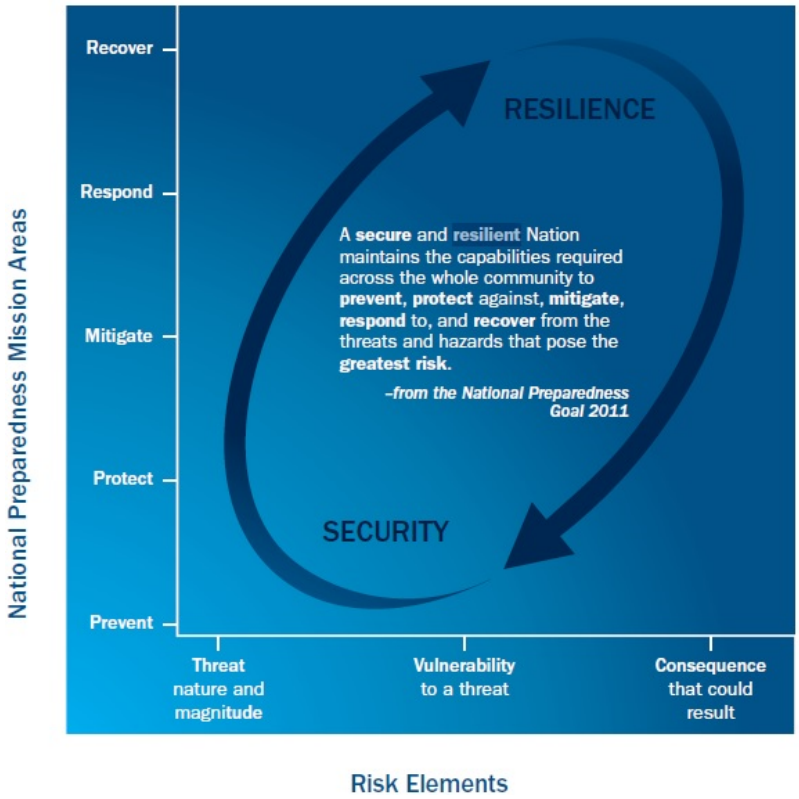


Figure 10. Security-Resilience Relationships. Source: NIPP 2013.

The NIPP 2013 emphasizes the importance of public-private sector partnerships in designing solutions for CIKR protection and resiliency. One organizational vehicle to meet the NIPP Goal is the Information Sharing and Analysis Centers. ISACs are sector owner/operator managed intelligence centers that provide real-time data gathering, analysis, and dissemination of sector-relevant threat analysis, incident reporting, and risk warning. The ISACs have the ability to purge proprietary information from reports to share with stakeholders within and across sectors, as well as with the government.[67] Many of the 18 recognized CIKR Sectors have ISACs; within the transportation sector is a maritime ISACs—the Maritime Security Council. The maritime ISAC should be more fully engaged in port security and could prove an extremely valuable tool for building maritime resiliency, port security, and MDA.

[67] DHS, "National Infrastructure Protection Plan 2013," 38.

Each Sector has a Sector Specific Plan (SSP). Figure 11 provides the Transportation Sector's Vision, Mission, and Goals statement from the NIPP 2013, Transportation Sector SSP:[68]

Vision	*A secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties.*
Mission	*Continuously improve the risk posture of transportation systems serving the Nation.*
Goals	*Prevent and deter acts of terrorism using, or against, the transportation system;* *Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests;* *Improve the effective use of resources for transportation security; and* *Improve sector situational awareness, understanding, and collaboration.*

Figure 11. NIPP Mission Statement and Goals. Source: NIPP 2013, Transportation Sector SSP.

The NIPP 2013 Transportation Sector SSP explicitly updated the Risk Model, with two variants: "Risks *to* the transportation system, and risks *from* the transportation system."[69] The first case modifies the former "threat" variable and now defines it as the "probability" that something may occur. It also defines risk as a function of that probability and the likely consequences, expressed as:

$$\textbf{Risk} = f\ \textbf{(Probability, Consequence)}$$

[68] Adapted from DHS, "National Infrastructure Protection Plan 2013 Transportation Sector Specific Plan," https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (accessed January 30, 2016).

[69] Department of Homeland Security, "National Infrastructure Protection Plan 2013 Transportation Sector Specific Plan," https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (accessed January 30, 2016).

The second equation assumes that the transportation systems itself, or elements of it, are weaponized and used against other targets. This second equation slightly modifies the traditional Risk Equations by, instead of multiplying Threat by Vulnerability by Consequence to determine the Risk, Risk is now considered a function of the three, notated in the following:

> Terrorist risks do not have a statistical basis for determining probability; therefore, the following alternate equation, developed by the Government Accountability Office in 2001, is typically used within the sector:
>
> **Risk = *f* (Threat, Vulnerability, Consequence)**[70]

8. Port Security Grant Program (PSGP) Guidance

Each year the PSGP administrator, currently the DHS-FEMA Grant Programs Directorate (GPD) is the administrator for the PSGP. For each fiscal year, the GPD announces the grants' open period with the publication of a Notice of Funding Opportunity (NOFO). Within the NOFO are the precepts, or guidelines, that applicants must follow in submitting grants proposals. The Guidelines state such things as eligibility criteria, application deadlines, submission procedures, and the application content (e.g., justifications, details, attestations, budget, and specifics of the proposal). The Guidelines also define what projects are eligible for funding, what the objectives and priorities for funding are for the current period, any cost-share provisions, and the details of specific supporting documentation that must accompany a complete proposal.[71]

Proposals go through a multi-step review process to ensure eligibility and determine the rank ordering of priority for awarding grant funding. The process is:

---

[70] DHS, "National Infrastructure Protection Plan 2013 Transportation Sector Specific Plan," 4.

[71] Department of Homeland Security. "Notice of Funding Opportunity Fiscal Year 2015 Port Security Grant Program (PSGP)," 1-17, http://www.fema.gov/media-library-data/1429282564066-3b452acb7dc7a2f1460a15ed855547d9/FY2015PSGP_NOFO_v2.pdf. (accessed January 7, 2016.

(1) First level review by FEMA GPD for eligibility and suitability—determine if the proposal meets the minimal requirements for consideration;

(2) COTP/AMSC Field Review—Then the AMSC provides the COTP with a preferred rank ordering of proposals, with the COTP making final judgments and recommendations as the Federal Maritime Security Coordinator (FMSC) to the next level of review;

(3) National Review Panel—The proposal is forwarded up, with priority recommendations, to Coast Guard Headquarters and FEMA for national level review; finally,

(4) DHS Headquarters makes a determination on final ranking and grant awards using risk-based review against the top-tier National Strategies and policy.

After the final review, a recommendation is made by FEMA to the DHS Secretary, who is the final approval authority for awarding grant funds to the winning proposal applicants.[72]

The PSGP process assumes a 360° cycle, with post-award reviews, lessons learned applied to developing the next fiscal year's PSGP Guidelines, and it starts over again. Over the life of the PSGP, there have been numerous changes. The grant administrator has changed three times, with the program residing for the longest duration within FEMA GPD, which currently retains administration. Other changes have been: a period of performance, eligibility criteria, project inclusions and exclusions, funding amounts, cost share requirements, port groupings, whether or not a fiduciary agent is required or if applications can come from consortiums, the specific areas of focus for the term, and many more variables.

[72] DHS, "Notice of Funding Opportunity Fiscal Year 2015 Port Security Grant Program (PSGP)," 17–28.

Figure 12 graphically represents the PSGP annual cycle.

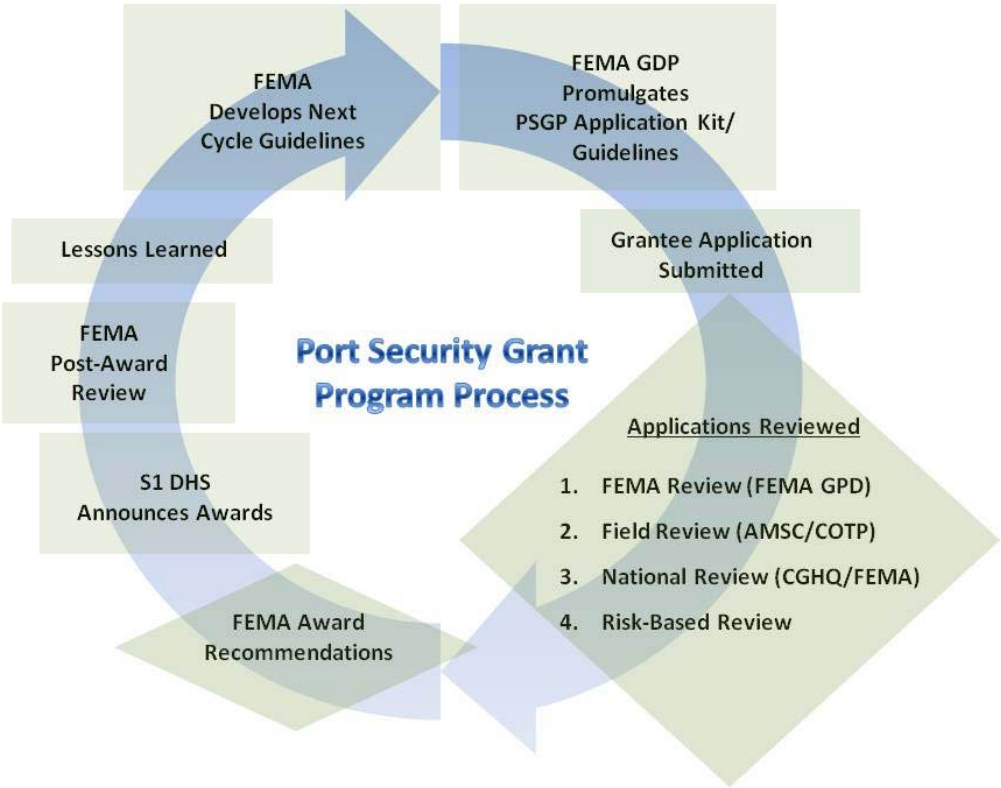


Figure 12. Port State Control Grant Process. Source: Notice of Funding Opportunity Fiscal Year 2015 Port Security Grant Program (PSGP).

The PSGP has undergone some changes over its lifetime. Originally the Department of Homeland Security (DHS) Office of Domestic Preparedness (ODP)[73] managed the PSGP as the 2003 Urban Areas Security Initiative (UASI) Port Security Grant Program (PSGP). "Although administered by the ODP, the UASI Port Security Grant Program [was] coordinated by the Transportation Security Administration (TSA)."[74] That first year the PSGP focused on providing

[73] ODP transferred to Department of Homeland Security from the Department of Justice in 2003.

[74] Department of Homeland Security, "The Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program," http://ojp.gov/archives/solicitations/docs/fy03uasi_psg.pdf (accessed January 10, 2016).

funding for only 14 specific ports and 14 specific expenditures:[75] See Figure 13 for the initial PSGP Ports and Eligible Expenditures published in the FY 2003 UASI Port Security Grant Program Notice of Financial Offer (NOFO).

Eligible Ports	Eligible Expenditures
New York/New Jersey	Personal Protective Equipment (PPE)
Los Angeles/Long Beach	Explosive Device Mitigation & Remediation Equipment
Seattle	CBRNE[76] Search & Rescue Equipment
Hampton Roads	Interoperable Communications Equipment
Miami	Detection Equipment
Houston	Decontamination Equipment
Philadelphia	Physical Security Enhancement Equipment
New Orleans	Terrorism Incident Prevention Equipment
Beaumont	CBRNE Logistical Support Equipment
Charleston	CBRNE Incident Response Vehicles
Port Canaveral	Medical Supplies & Limited Types of Pharmaceuticals
San Juan	CBRNE Reference Materials
Valdez	Patrol Vehicles, including Watercraft
Louisiana Offshore Oil Port (LOOP)	TSA Compliant Employee Identification Card System (i.e., TWIC[77])

Figure 13. Initial PSGP Ports and Eligible Expenditures. Source: FY 2003 UASI Port Security Grant Program NOFO.

The total funds available for assignment to successful proposals was $75,000,000. There was no matching requirement. Grantees were required to

[75] Adapted from DHS, "The Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program," http://ojp.gov/archives/solicitations/docs/fy03uasi_psg.pdf (accessed January 10, 2016).

[76] CBRNE = Chemical, Biological, Radiological, Nuclear, and Explosive.

[77] TWIC = Transportation Worker Identification Credential.

post financial status and program progress reports during the grant performance period. The private sector was ineligible to apply.

By 2005, the PSGP was a stand-alone grant program within the overarching suite of Homeland Security Grant Programs (HSGP), now managed by DHS' Office of State and Local Government Coordination and Preparedness (SLGCP), Office for Domestic Preparedness (ODP). The pot of money for distribution to successful PSGP proposal doubled to $150,000,000.[78] The PSGP Guidance aligned with the National Preparedness Goal established by Homeland Security Presidential Directive 8 (HSPD-8), which required that the PSGP align with the National Infrastructure Protection Plan (NIPP), and utilize the National Planning Scenarios,[79] the Universal Task List (UTL),[80] and Target Capabilities List (TCL).[81] The 2005 PSGP Guidelines increased the number of eligible ports to 66[82] and opened the competition up to private sector facilities and U.S. inspected vessels regulated by the MTSA, port authorities, and consortia comprised of either to also include port associations.[83] The risk-based allocations identified the ports to get funding using the Risk Equation (R = V*T*C),[84] the port areas were to choose the five best proposals for consideration by DHS.[85] Private sector stakeholders also had to provide 50% of the proposal cost. There were no matching funds required of public sector stakeholders. For

---

[78] Department of Homeland Security, "Fiscal Year 2005 Port Security Grant Program (PSGP): Program Guidelines and Application Kit," Forward, https://www.fema.gov/pdf/government/grant/psgp/fy05_psgp_guidance.pdf (accessed January 7, 2016).

[79] There are 15 National Planning Scenarios—12 Terrorist Attack Scenarios, 2 Natural Disaster Scenarios, and 1 Pandemic Disease Scenarios. The Scenarios are used as frameworks for developing planning strategies to protect against.

[80] The UTL are the tasks necessary to execute responses to the National Planning Scenarios at all levels of government.

[81] DHS, "Fiscal Year 2005 Port Security Grant Program (PSGP): Program Guidelines and Application Kit," 1. (The TCL is a set of 36 capabilities necessary to perform the UTL.)

[82] Ibid., 2.

[83] DHS, "Fiscal Year 2005 Port Security Grant Program (PSGP): Program Guidelines and Application Kit," 5.

[84] Ibid., 3.

[85] Ibid. 7.

FY 2005, there were 36 Target Capabilities List Critical Capabilities, listed in Figure 14.

Critical Capabilities

1. Animal Health Emergency Support	19. Isolation and Quarantine
2. CBRNE Detection	20. Mass Care (Sheltering, Feeding, and Related Services)
3. Citizen Preparedness and Participation	21. Mass Prophylaxis
4. Citizen Protection: Evacuation and/or In-Place Protection	22. Medical Supplies Management and Distribution
5. Critical Infrastructure Protection	23. Medical Surge
6. Critical Resource Logistics and Distribution	24. On-Site Incident Management
7. Economic and Community Recovery	25. Planning
8. Emergency Operations Center Management	26. Public Health Epidemiological Investigation and Laboratory Testing
9. Emergency Public Information and Warning	27. Public Safety and Security Response
10. Environmental Health and Vector Control	28. Restoration of Lifelines
11. Explosive Device Response Operations	29. Risk Analysis
12. Fatality Management	30. Search and Rescue
13. Firefighting Operations/Support	31. Structural Damage Assessment and Mitigation
14. Food and Agriculture Safety and Defense	32. Terrorism Investigation and Intervention
15. Information Collection and Threat Recognition	33. Triage and Pre-Hospital Treatment
16. Information Sharing and Collaboration	34. Volunteer Management and Donations
17. Intelligence Fusion and Analysis	35. WMD/Hazardous Materials Response and Decontamination
18. Interoperable Communications	36. Worker Health and Safety

Figure 14. Source: PSGP FY 2005, 36 Target Capabilities List Critical Capabilities.

In 2006, the funds level remained almost steady at $168,000,000. The PSGP was now administered by the Office of Grants and Training under the new Preparedness Directorate within DHS.[86] Grant proposals need to address the National Priorities cited in the National Preparedness Goal. The main focus for this iteration was on establishing means to defeat attacks with improvised explosive devices (IED).[87] The number of eligible ports was now up to 101, as

[86] Department of Homeland Security, "Fiscal Year 2006 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit," Forward, https://www.fema.gov/pdf/government/grant/psgp/fy06_psgp_guidance.pdf. (accessed January 7, 2016).

[87] Ibid., 2.

well as previously available to MTSA regulated facilities and U.S. inspected vessels, port consortia, and port authorities. Matching funds were required, with public sector stakeholders having to provide 25% of the proposal cost and private sector stakeholders having to provide 50% of the proposal cost.

The Fiscal Year 2007 PSGP Guidelines brought the grant program into compliance with the SAFE Port Act, expanding the group of eligible applicants to "all entities covered by an Area Maritime Security Plan (AMSP)."[88] In 2007, port areas were assessed risk profiles and identified by "tier,"[89] from Tier I through Tier IV, with Tier I being the highest risk.[90] The funding distinction allocated a set amount that each successful applicant within Tier I ports would be eligible for, and with Tier II through Tier IV ports competing for the pool of funds designated for their respective Tiers.[91]

By FY2007, FEMA's Grants Program Directorate (GPD) was responsible for administering all Homeland Security Grant Programs (HSGP), including the PSGP.[92] GPD opened avenues for "applicants to have consultations with the Department's grant program and subject matter experts."[93] The period of performance was established at 36 months, with the "largest portion of the port grant dollars … awarded to the highest risk facilities and for projects that offer the maximum return on investment for risk reduction."[94]

---

88 Ibid., i.

89 The term "Port Tiers" is later changed to "Port Groups" in FY2008.

90 DHS, "Fiscal Year 2006 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit," 1.

91 Ibid., 2–3.

92 Administration of the PSGP changed four times before residing in FEMA's GPD. GPD was determined by DHS to be the natural administrator for Departmental preparedness grants. The frequent transfer of the PSGP is largely an artifact of a newly formed and rapidly evolving Department of Homeland Security.

93 DHS, "Fiscal Year 2006 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit," i.

94 Ibid.

The FY2007 PSGP Guidelines emphasize target projects that increase "port-wide risk management, enhanced domain awareness, capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons, as well as training and exercises."[95]

Table 1 breaks down the primary similarities and changes between the remaining annual iterations of the PSGP Guidelines from FY2008 to FY20115.

PSGP Year	Port Groups	Funding Level ($Million)	Support Nat'l Preparedness System	Fiduciary Agent[0]	Consortia	Supports AMSC PRMP/BCRTP	Cost Matching Required	Perform-ance Period (Months)	Allowed Projects
2008[2]	I, II, III & All Others	$388.6	No	Yes	Yes	No	25% Public / 50% Pvt Sector (No Match Req'd for Proposals of ≤$25K	36	MDA, IDE, Training & Exercise, TWIC
2009[2]	I, II, III & All Others	$388.6	No	Yes	Yes	Must have PRMP; BCRTP Encouraged PSGP began shift from individ entities to port-wide risk	25% Public / 50% Pvt Sector & Consortia Cash or In-kind (No Match Req'd for Proposals of <$25K	36	MDA, IDE & WMD, Training & Exercise, TWIC
2010[2]	I, II, III & All Others	$438[4]	NIMS, but not specifically NPS	Yes	Yes	Must have PRMP; BCRTP Encouraged	None	36	IDE, MDA, TWIC, Training & Exercise
2011[2]	I, II, III & All Others	$235	NIMS, but not specifically NPS	Yes	Not excluded	Must have PRMP; BCRTP Encouraged	Waived	36	Same as 2010, plus Resiliency & Recovery
2012[2]	I, II, & III	$97.5	Yes	No	No	Must have PRMP; BCRTP Encouraged	25% Public / 50% Pvt Sector (No Match Req'd for Proposals of ≤$25K	24	Same as 2011
2013[2]	I & II (No Designated Ferry[3] Allocations)	$93	Yes	No	No	Encouraged to maintain.	25% Public / 50% Pvt Sector	24	Same as 2011, plus Cyber Security
2014[2]	I & II Only	$100	Yes	No	No	Encouraged to maintain.	25% Public / 50% Pvt Sector	24	Same as 2013
2015[2]	None. Competitive Review.	$100	Yes	No	No	Encouraged to maintain.	25% Pub/Pvt Waiverable	36	Same as 2013

[0]The Fiduciary Agent serves as the point of contact for administration and management of Group I & II ports' awards.
[2]Entities with outstanding or open Notice of Violations are ineligible to compete, except if certain conditions are met per the Guidelines.
[3]Ferry/ferry systems that applied for the FY 2013 Transit Security Grant Program (TSGP) are not eligible for PSGP grant funding.
[4]The $438,000,000 reflects $288,000,000 in FY2010 PSGP funding plus an additional $150,000,000 in port-specific grants from the Recovery Act.

Table 1. FY2008 through FY2015 PSGP Funding Guidelines.

95 Ibid., 1.

9. Government Accountability Office (GAO) Audits

Feedback for any endeavor is essential to improvement; external feedback from a neutral third party is even better. The United State Government Accountability Office has filled this role well throughout the life of the Port Security Grant Program, filing many reports that critique and offer corrective actions or additional areas for improvement in the PSGP. Over the almost decade and a half of the PSGP and the attendant GAO reports, there have been significant critiques and observed improvements in response. The GAO is politically neutral in their reports to Congress, providing succinct and value-added recommendations that, in turn, the Executive agencies (i.e., DHS, FEMA, USCG) have embraced for action and employed programmatic improvements to address the GAO critiques and recommendations to the degree they are capable.[96]

One recurring theme in the GAO reports cited the need to improve the risk equation, in particular about the vulnerability variable to account for differences between ports and changes due to enhancements, including those from PSGP grants.[97] In particular, GAO noted that the port security models being used to determine grant allocations did not account for reduced risk from funding prior grant proposals. Therefore, future port risk assessments cannot adjust for any improvement in a port's risk profile. No metric is available to measure the change in port risk profile. The absence of the ability to measure the effect of inputs—risk reduced from measures implemented since the prior port assessment—calls into question the accuracy of successive assessments.[98]

There frequently was concern about oversight and accountability to follow through on grantees fulfillment of the winning proposals, especially within the period of performance. Particularly frustrating for the GAO was the inability of

---

[96] GAO-12-47, 15–20.

[97] Ibid., 20.

[98] U.S. Government Accountability Office, *Maritime Security: Progress and Challenges with Selected Port Security Programs, Statement of Stephen L. Caldwell, Director, Homeland Security and Justice*, GAO 14-636T (Washington, DC, 2012), 10, http://www.gao.gov/assets/670/663784.pdf (accessed January 6, 2016).

FEMA to be aware of duplicative grant proposals across the suite of Homeland Security Grant Program (HSGP) grants (e.g., PSPG, UASI, and Transit Security Grants). Similarly, many proposals were designed so that their success was dependent upon winning multiple grants, such as a PSGP grant, a UASI grant, and perhaps a Firefighters Grant Program so that failure to successfully win all three grants would cause the entire project to fail.[99] The first concern relates to grantees getting double funding for a grant proposal.[100] The GAO suggests the grantees may hedge their bets by taking advantage of all opportunities. The other concern relates to large, complex proposals that have components of the proposal dependent upon the grantee winning grants from different sources.[101] The unease resolves around the risk of project failure if the project is unsuccessful in its bid for one or more of the dependent grants, leaving unspent funds that were unobligated for the successful grant applications. Both are legitimate problems to be solved.

In 2006, following Hurricanes KATRINA and RITA, the GAO recommended "DHS apply an all-hazards, risk management approach in deciding whether and how to invest in specific capabilities" for grant proposals.[102] Presidential Policy Directive 8 on National Preparedness (PPD-8), required the establishment of a National Preparedness Goal and a National Preparedness System.[103]

---

[99] U.S. Government Accountability Office, *Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress, Statement of William O. Jenkins, Jr., Director Homeland Security and Justice*, GAO 12-526T (Washington, DC, 2012) 4-11, http://www.gao.gov/assets/590/589446.pdf (accessed January 6, 2016).

[100] GAO 13-637T, 5.

[101] GAO 12-526T, 8.

[102] U.S. Government Accountability Office, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*, GAO 06-618 (Washington, DC, 2012), http://www.gao.gov/new.items/d06618.pdf (accessed January 6, 2016).

[103] *Presidential Policy Directive / PPD-8*—National Preparedness (Washington, DC: The White House, 2011), https://www.dhs.gov/presidential-policy-directive-8-national-preparedness (accessed October 11, 2015).

GAO expressed concern over a FEMA proposal for consolidating the disparate preparedness grants in its portfolio in the FY13 Presidential Budget Request to Congress. The goal was to simplify oversight and eliminate the potential for "double-dipping" or applying to multiple grants for the same proposal, or even depend upon multiple grants to complete a large project that is beyond the scope of any single grant. This proposal never became law but continues to be discussed.[104]

A final long-standing problem that the GAO has had with PSGP administration is with the frequency of the failure of grantees to meet the required milestones for disbursement of funds, leaving grant money tied up and unappropriated, while the clock runs down during the performance period.[105]

10. Congressional Research Service (CRS)

Much of the Congressional Research Service (CRS)[106] reports providing contextual information with course of action (COA) options for Congress to consider. In this regard, the CRS reports provide outstanding detail in insight into the history, definitions, details, and evolution of the program under review, as well as providing a set of options for improving them. The CRS reports provide perspective and a point of reference.

CRS Report "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress" (CRS RL33858) describes two relevant artifacts of risk: risk *management* and risk *inheritance*. Risk management is "a continual process or cycle in which risks are identified and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs

[104] GAO 12-526T, 11.

[105] GAO-12-47, 23-35.

[106] The CRS is a research service of the U.S. Library of Congress.

between risk acceptance and avoidance."[107] Risk inheritance refers to that risk assumed due to proximity to another at-risk entity. An example would be that a residential area outside the gates of a chemical facility would inherit risk from the facility; should a hazardous incident occur at the facility, it would impact the nearby community as well. Both of these concepts are directly applicable, and should be integrated into the process for assessing Port Security Grant proposals.

Another very interesting issue raised in CRS RL33858 is the quote from Secretary Chertoff that "federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support."[108] The report queries (a) whether grantees have come to view grants as entitlements; (b) if the PSGP could be discontinued at some point in time; and, (c) if metrics for determining if grant funds were being used as intended.[109] The report also alludes to finding synergies where the differing grant programs could share benefits, such as better intelligence sharing and analysis.[110]

CRS Report "Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress" (CRS R42683) suggests that the homeland security of critical infrastructure should advance from the defensive posture of infrastructure protection to the adaptive posture of building resiliency. Citing the Homeland Security Advisory Council's 2006 Report of the Critical Infrastructure Task Force, protection of critical infrastructure is seen as being a brittle strategy, whereas resiliency recognizes that adverse events may occur—some that may not be avoidable—but that building resiliency into critical infrastructure would

---

[107] U.S. Library of Congress, Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress,* by Todd Masse, Siobhan O'Neil, and John Rollins. CRS RL33858, 2007, 16 (accessed November 15, 2015 at http://fas.org/sgp/crs/homesec/RL33858.pdf).

[108] CRS RL33858, 2007, 27.

[109] Ibid.

[110] Ibid., 28.

minimize the impact and improve recovery.[111] The report discusses definitions of resilience/resiliency, some methods for measuring resiliency, and measures that could be taken to enhance resiliency.

The report further differentiates between protection and resiliency, "Perhaps a more useful way of making the distinction between protection and resilience is that protection focuses on the threat and resilience focuses on the consequences."[112]

11. Other Federal Reports

The 2006 report from the Homeland Security Advisory Committee's (HSAC) Critical Infrastructure Task Force (CITF) brought the discussion of *resilience* versus *protection* to the forefront. The CITF argued that current critical infrastructure protection (CIP) policy is heavily biased on protection measures, which are defensive in nature. "The CITF believes that protection, in isolation, is a brittle strategy."[113] Instead, the CITF proposed "making resilience the overarching strategic objective" of CIP, and that a by-product of building resiliency would be actions, plans, and processes that would positively impact the threat, vulnerability, and consequence variable of the Risk Model.

Driving their argument is the reality that it is impossible to protect every potential target against every possible threat—whether natural, accidental, or intentional. The CITF points out that it is impossible to determine when enough protection is enough against an infinite set of possible impact vectors. Instead, by offering building resiliency into the portfolio of CIP measures, strategies can be implemented that can rapidly restore critical infrastructure, diminishing the impact

---

[111] U.S. Library of Congress, Congressional Research Service, *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, by John D. Moteff. CRS R42683, 2012, Summary (accessed January 6, 2016) http://fas.org/sgp/crs/homesec/R42683.pdf).

[112] Ibid., 13.

[113] Department of Homeland Security, *Homeland Security Advisory Council: Report of the Critical Infrastructure Task Force,* https://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf, January 2006 (accessed February 10, 2016).

and rebounding more quickly. In the absence of resiliency, the effect from an unanticipated and undefended weakness could have an immediate and long-lasting impact. It goes on to suggest that the optimal risk mitigation portfolio would include both protective and resiliency enhancement measures.[114]

The 2014 Quadrennial Homeland Security Review (QHSR) identified five basic missions for the Department of Homeland Security for the next four years (2014–2018) when the next Quadrennial Review is due. Of these, Mission 5 most directly addresses the subject studied here, that being "*Strengthen National Preparedness and Resilience*."[115] The QHSR also injected another dimension of Risk looking forward: "The aging or deteriorating condition of significant aspects of [the United States'] critical infrastructure systems …."[116] The QHSR argues that the declining condition makes the CIKR more vulnerable by diminishing resiliency, potentially leading to adverse impacts greater than otherwise would be if the infrastructure were fully healthy.[117] However, the QHSR sees opportunity in the need to rebuild our infrastructure. In rebuilding, we can make the infrastructure more robust, more resilient, and able to better withstand the threats—natural, accidental, and intentional—that could disrupt the continuity of service it provides. There is a cost-benefit as well. By building resiliency into the infrastructure revitalization, direct construction costs could be spread across the project, which would certainly be less than having to rebuild devastated infrastructure.[118] QHSR speaks of "A Whole Community approach to planning and implementing disaster strategies,"[119] whereby stakeholder partnerships and relationships—between public and private sector entities—identify shared

---

[114] DHS, *HSAC: Report of the Critical Infrastructure Task Force.*

[115] Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review,* https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf, June 14, 2014, (accessed February 14, 2016).

[116] Ibid., 23.

[117] DHS, *The 2014 QHSR,* 23.

[118] Ibid., 24.

[119] Ibid., 74.

infrastructure concerns and seek common ground for improving the security and resiliency posture across that commonality.

The 911 Report noted that "[o]pportunities to do harm are as great, or greater, in maritime or surface transportation."[120] The 911 Report, therefore, recommended that "[h]ard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort."[121] With "[n]o single security measure [being] foolproof," building sufficient resiliency into CIKR to withstand disruptions, rather than focusing on specific threat vectors, will guarantee a return on investment greater than simply protecting the CIKR against a possible threat.[122]

B. ACADEMIC, RESEARCH, AND WHITE PAPERS

The remaining literature reviewed included academic papers, research, studies, reports, and white papers from academia, "think tanks," governmental agencies, consensus organizations, and students. The content of the literature included analytical models, statistical analysis, critiques, and studies that could potentially inform the discussion on the Port Security Grant Program.

Statistical data provided by industry organizations including the American Association of Port Authorities (AAPA), governmental agencies such as the Maritime Administration (MARAD), U.S. Army Corps of Engineers (USACOE) and research performed under the contract. Academic literature sought to explore potential models for assessing port security, critiques of the PSGP efficacy, studies of and alternatives to infrastructure protection, concepts of resiliency, and concepts of complexity and system of systems.

---

[120] National Commission on Terrorist Attacks (2011-05-16), The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States ("911 Report," Authorized Edition) (p. 391). W. W. Norton & Company. Kindle Edition.

[121] 911 Report, 391.

[122] 911 Report, 392.

In a 2005 report for the American Enterprise Institute, Veronique de Rugy, cut to the chase and raised the difficult point: "Since the number of possible attacks is effectively unlimited and the resources we can devote to the fight against terror are limited, spending should not occur without a careful cost-benefit analysis."[123] She makes an honest point. When facing limited resources for unlimited potential disruptive vectors (let us expand the concern beyond terrorism to include natural and accidental man-made disruptions), investments must be made that have the greatest promise of success in mitigating the highest probability of occurrence, weighted for severity of the impact. She emphasizes terrorist pose two threats to port security; (a) threat to the port, intending to disrupt maritime commerce, and (b) the threat through the port, by moving dangerous materials into the country for use in terror attacks (be they CBRNE/WMD, financing, small weapons). In discussing direct port threats, Ms. Rugy identifies the clear weakness in taking the "hardening of infrastructure" posture; the attacker has the inherent advantage of mobility, the ability to go around the hardened target and select another.[124] Ms. Rugy, therefore, determines that there be two avenues that best mitigate the terrorist risk to maritime ports: the first is, given the terrorist advantage of flexibility, intelligence gathering is the most cost-effective means of preventing an attack; "[t]he second-best solution is to mitigate damage after an attack."[125] She raises the concept of "mega port," those extremely large, complex port systems that coincide with major metropolitan population centers and multimodal transportation hubs through which the majority of the nation's trade flows. By definition, disruptions to mega ports would set off cascading impacts on a global scale with severe national economic damage.[126] Interestingly, her conclusion is to leave direct protection to the local authorities and CI owner/operators and leave the

---

[123] Veronique de Rugy, "What Does Homeland Security Spending Buy?," "What Does Homeland Security Spending Buy?," *AEI Economic Policy Working Paper Series* (2005): 3.

[124] de Rugy, "What Does Homeland Security Spending Buy?," 5.

[125] Ibid.

[126] Ibid., 6.

prevention of attack and interdiction of smuggling to national intelligence gathering.[127]

> Natural and human-induced disasters affect organizations in myriad ways because of the inherent interconnectedness and interdependencies among human, cyber, and physical infrastructures, but more importantly, because organizations depend on the effectiveness of people and on the leadership they provide to the organizations they serve and represent. These human-organizational-cyber-physical infrastructure entities are termed system of systems.[128]

Haimes provides insight into the understanding *system of systems* thinking and relevance for applying the theory to the maritime transportation system (MTS) as such. He describes concepts of "interdependent and interconnected subsystems, which in their totality constitute a system of systems."[129] He states that to model a complex system of systems, one must:

- Determine component system properties.
- Identify the relationships between the components and subsystems.
- Quantify Intra- and interdependencies between the core components and subsystems.
- Define the relational parameters and functions within the complex of component subsystems.[130]

A practical advantage of studying the MTS regarding a complex system of systems is the ability to understand the concepts of *coupling* and *emergence*, and how they influence system *disruption* and *resiliency*.[131] Haimes also speaks

---

[127] de Rugy, "What Does Homeland Security Spending Buy?," 13.

[128] Yacov Haimes, Joost Santos, Kenneth Crowther, Matthew Henry, Chenyang Lian and Zhenyu Yan. "Chapter 21: Risk Analysis in Interdependent Infrastructures," *Risk Analysis*, v.32, No.11, (2012): 1.

[129] Haimes, "Chapter 21: Risk Analysis in Interdependent Infrastructures," *Risk Analysis*, 1836.

[130] Haimes, "Chapter 21: Risk Analysis in Interdependent Infrastructures," *Risk Analysis*, 1836.

[131] Haimes, "Chapter 21: Risk Analysis in Interdependent Infrastructures," Risk Analysis, 1838.

to seeking a balanced approach to homeland security preparedness. Specifically, that "[b]alancing protective and resilience actions through system-level analysis will provide a means to improve the overall efficiency of regional and national preparedness."[132]

An important distinction "of the system of systems perspective is not prediction …, but instead is an understanding that the essence of the problem—the hard-to-grasp insight—likely appears only from this elevated perspective." Instead, the system of systems thinking seeks to understand "probability of possibilities, a 'what-if' map" in large complex, interdependent, and emergent systems.[133] Additionally, Haimes offers "[t]he system of systems performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire system of systems and not the behavior of any component system. The principle purposes supporting the engineering of these systems are fulfilled by these emergent behaviors."[134] Haimes further defines emergent systems as "those system features that are not designed in advance, but evolve, based on sequences of collected events that create the motivation and responses for properties that ultimately emerge into system features."[135] Emergence in systems are those evolutionary adaptations that are products of the relationships between subsystem components of a complex system that result in outcomes not anticipated or designed.

There have been criticisms of how the federal government has prosecuted national preparedness for all-hazards emergencies. Those criticisms are not the

---

[132] Yacov Y. Haimes, Kenneth Crowther, and Barry M. Horowitz, "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems," Center for Risk Management of Engineering Systems, University of Virginia, Published online 16 June 2008 in Wiley InterScience: DOI 10.1002/sys.20101, 287.

[133] D. DeLaurentis, R. K.Callaway, "(2004), A System-of-Systems Perspective for Public Policy Decisions. Review of Policy Research, 21: 829–837, doi:10.1111/j.1541-1338.2004.00111.x, 2.

[134] Haimes, "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems," 289.

[135] Haimes, "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems," 289.

sole province of the GAO. In the October 2008 edition of Homeland Security Affairs, Dr. Samuel Clovis challenges the DHS top-down model of policy creation, goal definition, and all-hazards preparedness, instead offering the contrapositive position:[136]

- There is no idealized level of national preparedness universally possible now or into the future with current resource levels;
- Successful fulfillment of grant fund policies is not dependent upon narrowly-defined, coercive and explicit direction from the federal government.
- Federally mandated homeland security, all-hazards preparedness cannot create a universally employable model across all jurisdictions.[137]

Since 9/11, the homeland security discussion has evolved from protecting critical infrastructure (CI) from terrorist attacks to making CI more resilient to all hazards disruptions. In this context, "resilience can be seen as having the ability to resist, absorb, recover from or adapt to adverse changes."[138] Kimmance makes the argument that, building resilience into an infrastructure system would dramatically improve sustainability and survivability. "A resilient infrastructure may be considered as one in which the physical systems and assets have a degree of robustness and are therefore capable of surviving and performing well under conditions of change while avoiding excessively conservative design."[139] Kimmance provides another description of what is meant by *interdependency*; "… infrastructure systems … are individually complex and comprise a collection of internally interacting components, as well as external linkages to other systems … [that] can bring synergies improving efficiency and service levels with associated economic and societal benefits."[140] It is important to emphasize that

---

[136] Samuel H. Clovis, Jr., "Promises Unfulfilled: The Sub-Optimization of Homeland Security National Preparedness," Homeland Security Affairs, v. IV, no. 3, October 2008, 18.

[137] Ibid., 1.

[138] James Peter Kimmance and Anthony John Harris, "Infrastructure Risk and Resilience: A Review," *The Institution of Engineering and Technology*, 2013, 9.

[139] Kimmance and Harris, "Infrastructure Risk and Resilience," 9.

[140] Ibid., 11.

unlike hardening and protection, which is defensive in posture and focuses on a specific, anticipated threat vector, resiliency seeks to make the infrastructure more robust and able to withstand unspecified threats by addressing uncertainty.[141]

Resilience in emergent systems is influenced by the coupling of the component subsystems of the system of systems. Redundancy and robustness are elements that help determine the resiliency of a system. Redundancy refers to the ability of other subsystem components to assume the lost or diminished capability and capacity of a damaged subsystem component. Robustness refers to the ability of a subsystem component to absorb impact, or of the system of the systems to withstand disruption.[142]

In ""A Systems Approach to Governance in Maritime Transportation System of Systems (MTSoS)" by Mo Mansouri et al. of Stevens Institute of Technology, they put forward the proposition that "[s]ince disruption as a result of uncertainty is inevitable, such systems need to be designed and operated in such a manner that they can adopt appropriate strategies such as flexibility, resilience, and agility in the face of disturbances."[143] Mansouri discusses the independence and interdependency of MTSoS constituent components as independent of one another, but at certain subsystem level are interdependent upon one another, making connections both hierarchically as well as horizontally, forming the complexity of the MTSoS.[144] Prime among the MTSoS constituents, according to Mansouri, are ships, ports, intermodal interfaces, the waterways, and users.[145] The elements of the MTSoS are influenced by laws, regulations, and policies;

---

141 Ibid.

142 Haimes, "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems," 291.

143 Mo Mansouri, Alex Gorod, Thomas H. Wakeman, and Brian Sauser, "A Systems Approach to Governance in Maritime Transportation System of Systems," *School of Systems and Enterprises, Stevens Institute of Technology*, Hoboken, 2009: 2.

144 Ibid.

145 Ibid., 3.

financial pressures; human and environmental factors—all who shape the response of the constituent elements and influence the emergence of the MTSoS.[146]

C. OTHER SOURCES

1. Stakeholders Survey

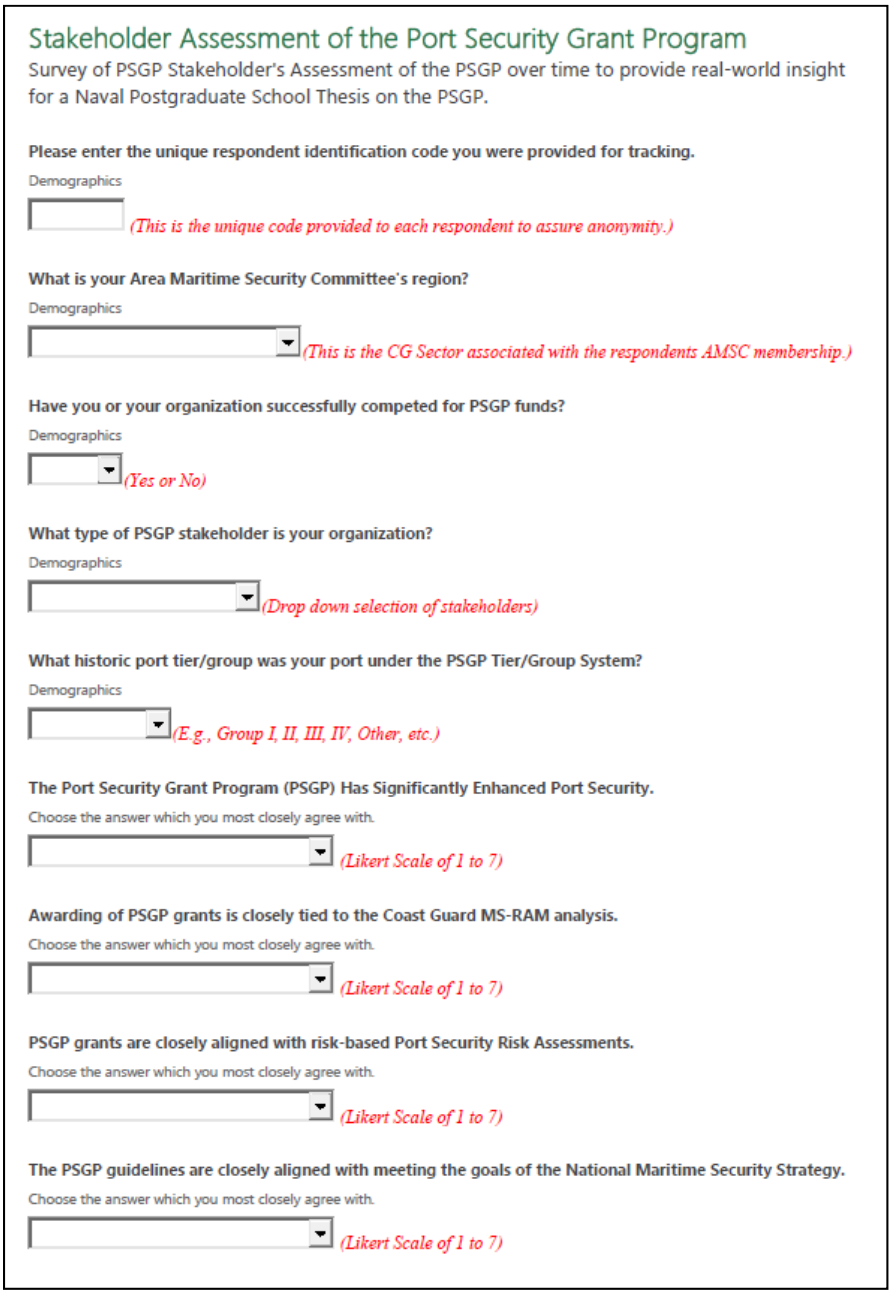
Port Security Grant stakeholders were recruited to participate in a short survey in addition to the review of literature and doctrine. The pool of potential respondents were members of two Area Maritime Security Committees (AMSC); one from an historically Tier I port, and the other from a Tier II port. Public and private sector MTS stakeholders comprise the AMSC membership. Their participation was crucial to understanding the PSGP from the stakeholders' points of view—the applicants, facilitators, and administrators. Their contributions provided insight into what the administrators believed was the purpose of the PSGP and how well it was meeting that purpose, and compared to the impression and experiences of the applicants and field-level stakeholders.

Potential survey respondents were recruited through their Coast Guard Sector Port Security Specialist by email. A consent form was provided, that explained details of the study and request to participate in the survey. AMSC members wishing to participate emailed signed forms back to the researcher, and in return were provided with a unique, randomly generated five-digit identification code and the survey in Excel format. The only identifier on the survey is the unique code. Only the researcher has the key to the code, kept on encrypted media, to preserve respondent anonymity.

The survey consisted of twenty questions. The first five were demographic in nature. The remaining was specific to the respondent's experience with the PSGP. The respondent was asked either to select a multiple choice answer, select "Yes" or "No," or identify their strength of agreement with a statement on a

[146] Ibid., 4.

7-point Likert Scale with 1 being Strongly Disagree to 7 being Strongly Agree. The survey questions are below, with the type of solution to the question in RED to the right. Figures 15 through 17 are screen captures of the survey.



Stakeholder Assessment of the Port Security Grant Program

Survey of PSGP Stakeholder's Assessment of the PSGP over time to provide real-world insight for a Naval Postgraduate School Thesis on the PSGP.

Please enter the unique respondent identification code you were provided for tracking.

Demographics

(This is the unique code provided to each respondent to assure anonymity.)

What is your Area Maritime Security Committee's region?

Demographics

(This is the CG Sector associated with the respondents AMSC membership.)

Have you or your organization successfully competed for PSGP funds?

Demographics

(Yes or No)

What type of PSGP stakeholder is your organization?

Demographics

(Drop down selection of stakeholders)

What historic port tier/group was your port under the PSGP Tier/Group System?

Demographics

(E.g., Group I, II, III, IV, Other, etc.)

The Port Security Grant Program (PSGP) Has Significantly Enhanced Port Security.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Awarding of PSGP grants is closely tied to the Coast Guard MS-RAM analysis.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

PSGP grants are closely aligned with risk-based Port Security Risk Assessments.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

The PSGP guidelines are closely aligned with meeting the goals of the National Maritime Security Strategy.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Figure 15. Survey Page 1.

Consolidation of the PSGP under an umbrella Homeland Security Grant Program would be good for continuing to enhance port security.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

The disallowance of consortiums to compete for the PSGP has had a positive impact on improving port security.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Port Security could be better served if AMSCs could compete for PSGP grants to fulfill gaps in Area Maritime Security Assessments and their respective Area Maritime Security Plans instead of individual port stakeholders competing against one another.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Other financial offsets could be as effective for promoting private sector investment in improved security, such as proportional tax deductions for security investments that meet the goals of the National Maritime Security Strategy.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Private sector offsets would be more equitable and expedite port-wide enhancement of securing the private sector portion of the port system than competing for PSGP grants.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

The PSGP grants should be designed to enhance the port or maritime transportation system (MTS) as a system, rather than as a collection of individual entities.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Performance periods for awarded grant proposals should be flexible rather than for rigid 1, 2, or 3 year periods.

Choose the answer which you most closely agree with.

(Likert Scale of 1 to 7)

Has your AMSC developed a Portwide Risk Mitigation Plan (PRMP) &/or Business Continuity/Resumption of Trade Plan (BCRTP)?

(Yes or No)

Does your AMSC actively collaborate with other regional security working groups, such as UASI groups and Transit Security Working Groups?

(Yes or No)

Figure 16. Survey Page 2.

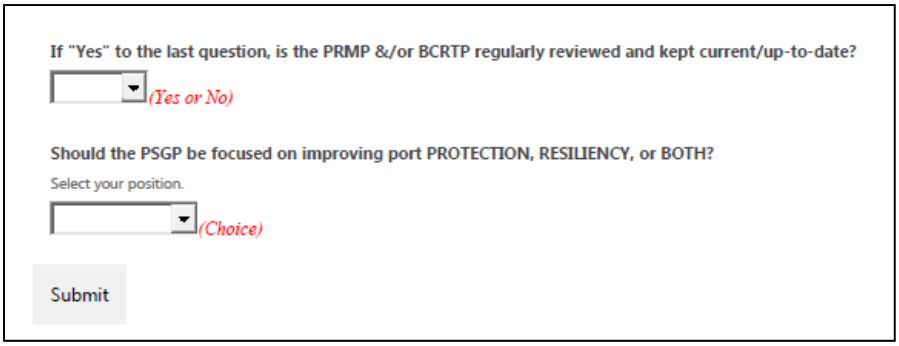


Figure 17. Survey Page 3.

2. Stakeholder Interviews

Finally, a selection of subject matter experts was interviewed to provide depth to the survey results. Some interviewees were members of the survey respondent cadre while others were program managers at FEMA GPD and U.S. Coast Guard Port Security Specialists and Coast Guard Headquarters program managers for MS-RAM and the Port Security Grant Program.

While the literature and survey results helped initiate the discussion, the direction of the conversations largely was left to the interviewees discretion with the only caveat to staying on the topic of the Port Security Grant Program. The interviews provided actual, first-person experience with the PSGP and well-validated preliminary conclusions drawn from the literature and surveys.

IV. ANALYSIS

A. FINDINGS FROM LITERATURE REVIEW

Despite the shock of the September 11, 2001, terrorist attacks, the United States federal government responded energetically. Beyond the horror of the human toll, the vulnerability and the vital need to protect our critical infrastructure and key resources was immediately recognized in the aftermath. That recognition included the profound understanding of how essential the nation's MTS is to our economic vitality, and how exposed the United States is to attacks to and through that vector. The directives, laws, regulations, policies, strategies, and plans that cascaded from the initiative to shore up our vulnerable MTS are well designed to support one another throughout the doctrine hierarchy. Each level of policies, plans and strategies support fulfillment of a strategic goal from the most macro level National Maritime Security Plan, through the Area Maritime Security Plans, down to the individual Vessel Security Plans and Facility Security Plans. The full suite of maritime security doctrine provides a clear and identifiable set of goals for targeting Port Security Grant Program funding application proposals; proposals that in turn complete the maritime security continuum from the national level to port level and individual stakeholders. The NIPP provides the foundation for developing CIKR protection strategies and making the CIKR more resilient when disruptions occur.

The PSGP has evolved over almost a decade and a half, shifting administrators to reside ultimately within FEMA's Grant Programs Directorate (GPD). Each year a Notice of Funding Opportunity (NOFO) is published by FEMA GPD that announces the PSGP's guidelines. The guidelines are ever evolving from one fiscal year to the next, however all proposals are required to adhere to the National Preparedness System and Goal.

These changes in protection strategy reflect the evolving understanding that the impact from disruption to critical infrastructure is the same regardless of

the cause. That is the point of having “lessons learned”—to learn from them, adapt, and improve in time for the next challenge against the system.

The GAO repeatedly calls out the need for FEMA to curb potential areas of waste, recommends consolidation of all Homeland Security Grant Programs into a single grant, and establish a means to measure how successful any given PSGP grantee proposal has been towards meeting its stated goal and improving port security. These include the lack of a mechanism for revising a port’s risk profile to account for risk mitigated through implementation of prior grant proposals; concerns about inefficiencies and potential waste when grant applicants compete for multiple, comparable grants, e.g., PSGP and Urban Area Security Initiative (UASI) grants. Also, the GAO cites the lack of progress in establishing Interagency Operations Centers (IOC)[147] mandated by the SAFE Port Act.[148] Lastly is the frequent inability of FEMA to disburse grant funds due to the failure of grantees to meet requisite project milestones.[149]

The 911 Report was focused primarily on the external, existential threat from terrorists and their stated desire to target disruption of our economic system. By publication of the 2014 QSHR the United States had experienced some natural and man-made disasters: Hurricanes KATRINA, RITA, and SANDY, as well as the Deepwater Horizon Oil Rig disaster. The evolution from terrorist-centric to all-hazards focused planning heralds the maturation of the homeland security field of play. The National Response Plan evolved into the National Response Framework, with a suite of Frameworks underpinning the complete planning and response life cycle. As such, the 2014 QSHR strongly emphasized the dual importance of protection AND resiliency as necessary ingredients for shoring the nation’s critical infrastructure from disruptive and perhaps debilitating impact from all hazards.

---

[147] GAO 14-636T, 6.

[148] IOCs are envisioned as port-wide, MTS-centric interagency fusion centers that provide real-time Maritime Domain Awareness (MDA) and Common Operating Picture (COP) for the region they support and collaborative response coordination to port threats.

[149] GAO-12-47, 23-35.

From the CRS come important concepts to consider in assessing port risk and building risk management strategies:

- Risk inheritance—risk assumed from proximity to another at-risk entity.
- Risk management—a continual process of risk identification and monitoring to inform decisions for risk acceptance and avoidance.[150]
- Asset protection is a brittle strategy; resiliency strategies would minimize the impact and improve recovery.[151]
-

> *"Perhaps a more useful way of making the distinction between protection and resilience is that protection focuses on the threat and resilience focuses on the consequences."*[152]

I concur with the recommendation to incorporate both concepts in any assessment for Port Security Grant proposals.

The CRS also highlighted a key concern of then Secretary Chertoff; that "federal homeland security assistance should not remain a program for general revenue sharing."[153] Financial dependency is always a concern with grant programs. State, local and tribal jurisdictions often look to grants as budget supplements—they may even plan their operational budgets with the expectation of being awarded grant funds. The CRS suggested that larger, more complex projects could benefit from building synergies between multiple grants, the GAO sighted the lack of visibility of inter-grant applications and project dependencies on multiple grants as problematic. There is a fine line between gaining synergies by stacking multiple grants to fulfill larger, complex projects, and the risk of project failure if the grantee failed to compete for a dependent grant. Additionally,

---

[150] CRS RL33858, 16.

[151] DHS, *HSAC: Report of the Critical Infrastructure Task Force.*

[152] CRS R42683, 13.

[153] CRS RL33858, 16.

without sufficient oversight of the entirety of grants applied for, there is a risk for waste and mismanagement.[154]

The CRS' key concept is that it is time for critical infrastructure protection to shift from simply protecting CI to ensuring that CI is more resilient and better able to recover quickly from disruptive events.[155]

While doctrine has been updated to include "resiliency" as a CI risk management strategy, the initiative has not translated sufficiently into the PSGP guidance. Resiliency remains a vague concept, and in practice, while the PSGP continues to focus on awarding individual grant proposals, the resiliency of the MTS as a system of systems cannot be realized.

The Homeland Security Advisory Committee's (HSAC) Critical Infrastructure Task Force (CITF) amplified the CRS' call to not only embrace resiliency as a critical component of CI risk management strategies but elevate systemic resiliency as a priority over protection. The logic is that "The CITF believes that protection, in isolation, is a brittle strategy."[156] That assessment hinges on the determination that current critical infrastructure protection (CIP) emphasizes protection measures, such as hardening individual entities, which is defensive in nature and fails to address continuity of operations during and after an incident.[157]

The 2014 Quadrennial Homeland Security Review (QHSR) identified five basic missions for the Department of Homeland Security for the next four years (2014–2018). Mission 5, "*Strengthen National Preparedness and Resilience*"[158] elevates resiliency building as a national preparedness priority. The QHSR adds the "deteriorating condition" of our CI as contributing to the vulnerability of our CI

---

154 Ibid., 27.

155 CRS R42683, Summary.

156 DHS, *HSAC: Report of the Critical Infrastructure Task Force.*

157 Ibid.

158 DHS, *The 2014 QHSR,* 14.

to disruptive impacts[159] due to the inherently reduced resiliency and potentially greater impact from disruption than would be otherwise. The QHSR then offers a silver lining; investing in CI rehabilitation now could incorporate improvements to resiliency at less cost than if investing in resiliency enhancements retroactively and alone.[160] The QHSR also addresses a "Whole Community approach to planning and implementing disaster strategies;"[161] a perspective that would welcome consortiums of port stakeholders to work together to enhance port security and resiliency.

The 911 Report's highlighting of the significant damage to the nation that could be realized through the MTS vector, either directly against the MTS or taking advantage of the MTS to further infiltrate the country and do harm elsewhere, is significant.[162] The maturation of homeland security strategy since then has evolved from the defensive protection posture to the denial or limitation of success posture of building resiliency into the CI. The "hard choices" the 911 Report referred to in determining how best to invest limited resources is in part mitigated by building in resiliency. Resiliency, by definition, buys down risk.[163] After all, "[n]o single security measure is foolproof."[164]

B. FINDINGS FROM SURVEYS

The participation rate was disappointingly low and insufficient to make statistically supportable inferences. However, given the fairly even distribution of representatives from the various stakeholder communities, some patterns emerged, supported by the follow-up and more detailed interviews, to sufficiently develop broad and useful conclusions.

---

159 Ibid., 23.

160 DHS, *The 2014 QHSR,* 23-24.

161 Ibid., 74.

162 911 Report, 391.

163 Ibid.

164 Ibid., 392.

From the survey results, the respondents clearly ascribe value to the PSGP, regardless of their role or association within the MTS—public or private sector affiliation. While there is agreement that the PSGP guidelines correlate with the National Strategy for Maritime Security, the PSGP linkage with the MS-RAM analyzes and AMSC Port Security Risk Assessments is spurious at best, with respondents reporting “Strongly Disagree” to “Strongly Agree” on the related questions asserting close linkages.

Universally, no respondents believed that it would be better to roll the PSGP into a single homeland security grant. Similarly, it was also unanimously felt that port consortiums should be allowed to compete for PSGP funds. There was strong, positive agreement that the PSGP could be improved if PSGP funding focused on holistic port-wide security improvements rather than through a patchwork of individual port entities competing against one another for funding.

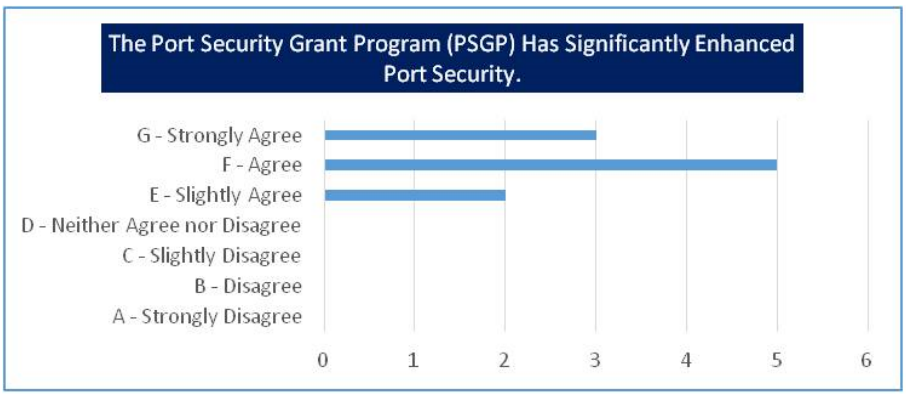
Respondents were not enthusiastic about either of the alternative funding proposals of tax deductions or other fiscal offsets to encourage the private sector to self-invest in enhancing their private infrastructure security, protection, and resiliency.

One interesting result was that all but one respondent either disagreed or had a neutral stance on the suggestion that flexible performance periods should replace rigid one, two, or three-year periods. The expectation was that greater flexibility in meeting project milestones would be desirable.

Both AMSCs had developed Port-wide Risk Mitigation Plans (PRMP) and Business Continuity/Resumption of Trade Plans (BCRTP) and periodically review and update them. Of the two, only the smaller, Tier 2 port AMSC actively collaborate with other regional security groups outside the AMSC, such as with UASI-only or Transit Security Working Groups. All but one respondent thought that both protection and resiliency should be the focus of PSGP projects; that one outlier felt only protection should be the focus.

The statement about *"The disallowance of consortiums to compete for the PSGP has had a positive impact on improving port security"* were all either neutral or in disagreement with that statement. However, there was a dual mode result, with one modal peak at the one extreme of "Strongly Disagree" and the other at the opposite end of the respondent spectrum of "Neither Agree nor Disagree." Looking deeper at the data, the respondents that *Strongly Disagreed* are from a Tier I port encompassing three States, a Top 5 metropolitan city, a Top 10 port system, and two Federal Regions. Despite those challenges, or because of them, there was a strong belief that consortiums were valuable to improving port security through the PSGP. It is also noteworthy that the respondents in this group represented Federal, State agency, and private sector respondents. The second modal peak for the Tier II port respondents represented the same stakeholder grouping: Federal, State, and Private Sector. However, the Tier II port is small, homogeneous, and wholly within the boundaries of a single state and single Federal Region.

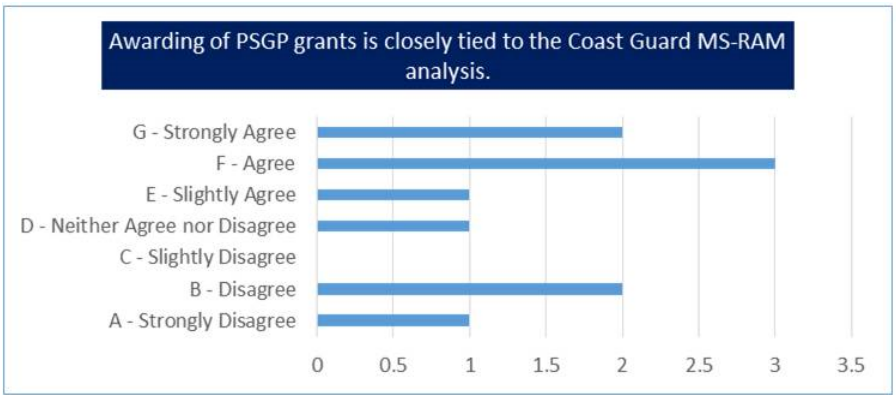
The following graphs in Figures 18 through 21 show the distribution of answers for each Likert Scale question, with Tables 2 and 3 displaying raw data.



Interpretation:

- 100% of the respondents concurred that the PSGP has significantly enhanced port security.

StdDev = 0.738
Mode = F

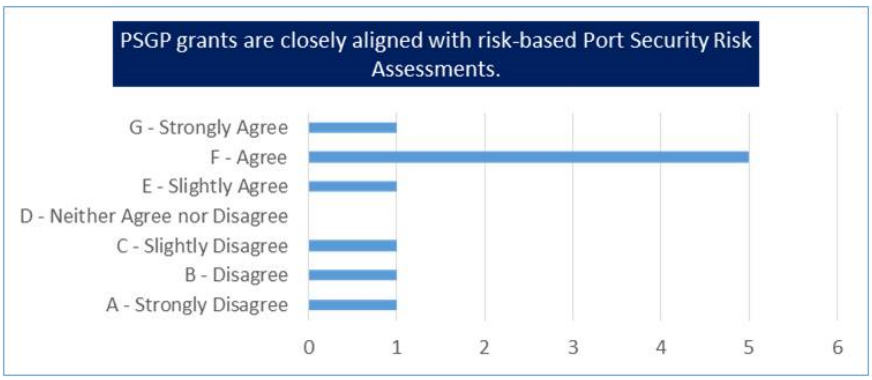


Interpretation:

- There is a slight tendency to agree that the PSGP and MS-RAM are closely related, but it is worth looking more closely to see if there is indeed a relationship.

StdDev = 2.221
Mode = F

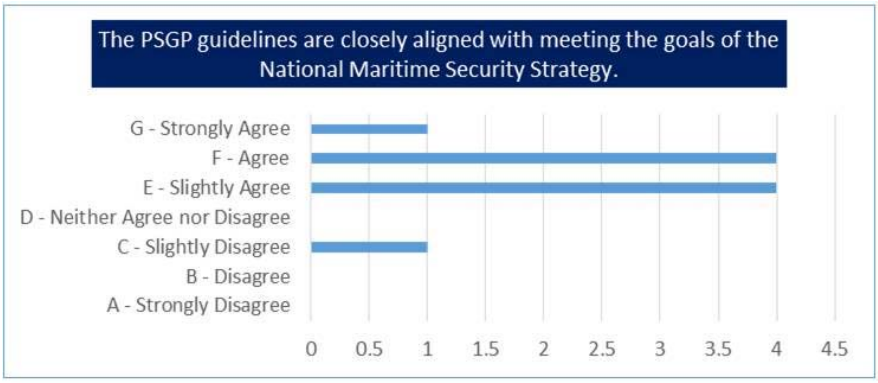
Figure 18. Survey Results.



Interpretation:

- The modal tendency is concurrence that the PSGP grants are aligned with the Port Security Risk Assessments.

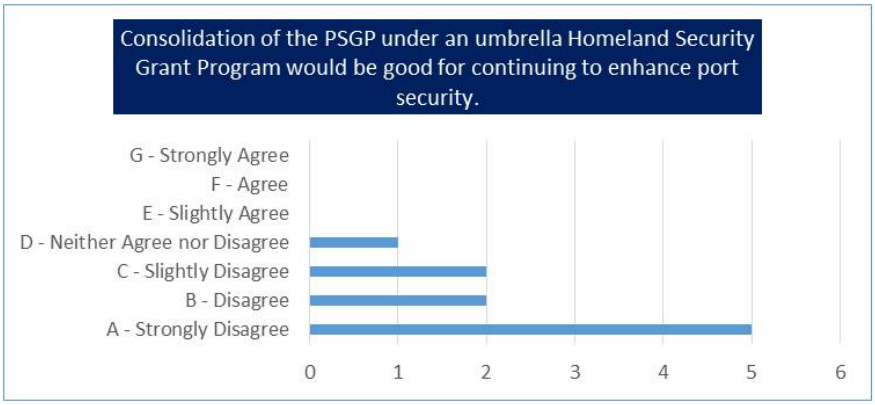
StdDev = 2.044
Mode = F



Interpretation:

- The modal tendency is concurrence that the PSGP grants are aligned with the Port Security Risk Assessments.

StdDev = 1.075
Mode = E/F

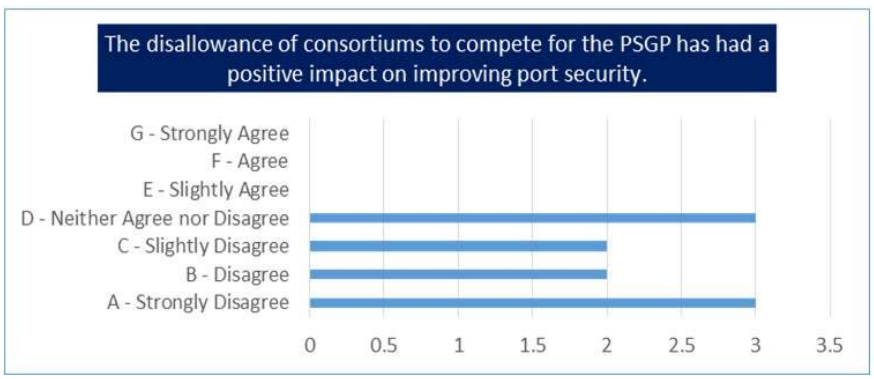


Interpretation:

- There is unanimity against consolidation of the PSGP into a single Homeland Security Grant Program; the PSGP must remain MTS-specific.

StdDev = 1.101
Mode = A

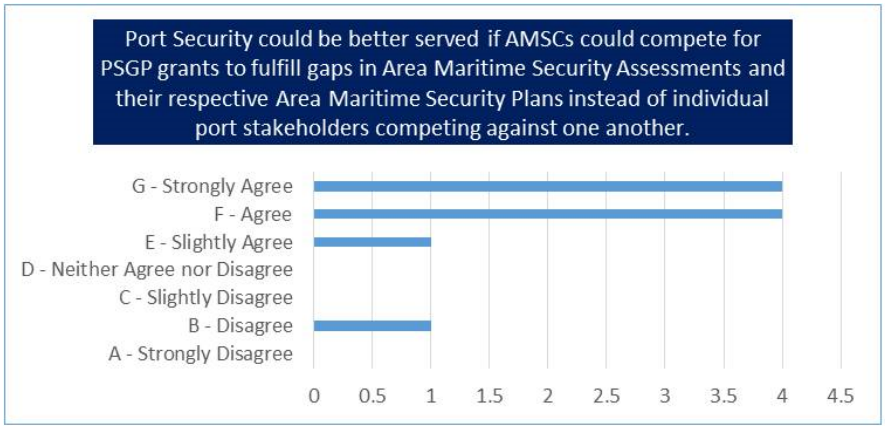
Figure 19. Survey Results.



Interpretation:

- Universally, all respondents felt that consortiums should be allowable to compete for PSGP grants in some fashion.

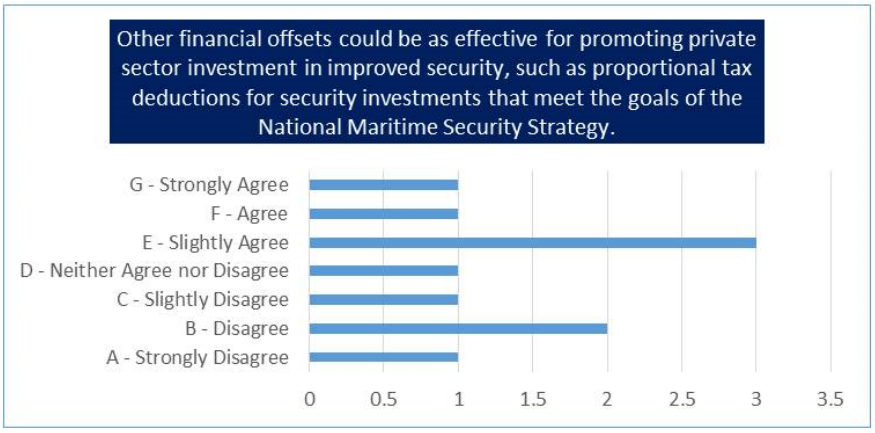
StdDev = 1.269
Mode = A/D



Interpretation:

- High agreement that PSGP grant proposals should be focused on filling gaps in the AMSP/PRMP rather than individual stakeholders gaps.

StdDev = 1.524
Mode = F/G



Interpretation:

- No consensus on how to best incentivize enhancing port security/resiliency to meet the National Maritime Security Strategy outside of PSGP grant awards.

StdDev = 1.944
Mode = E

Figure 20. Survey Results.

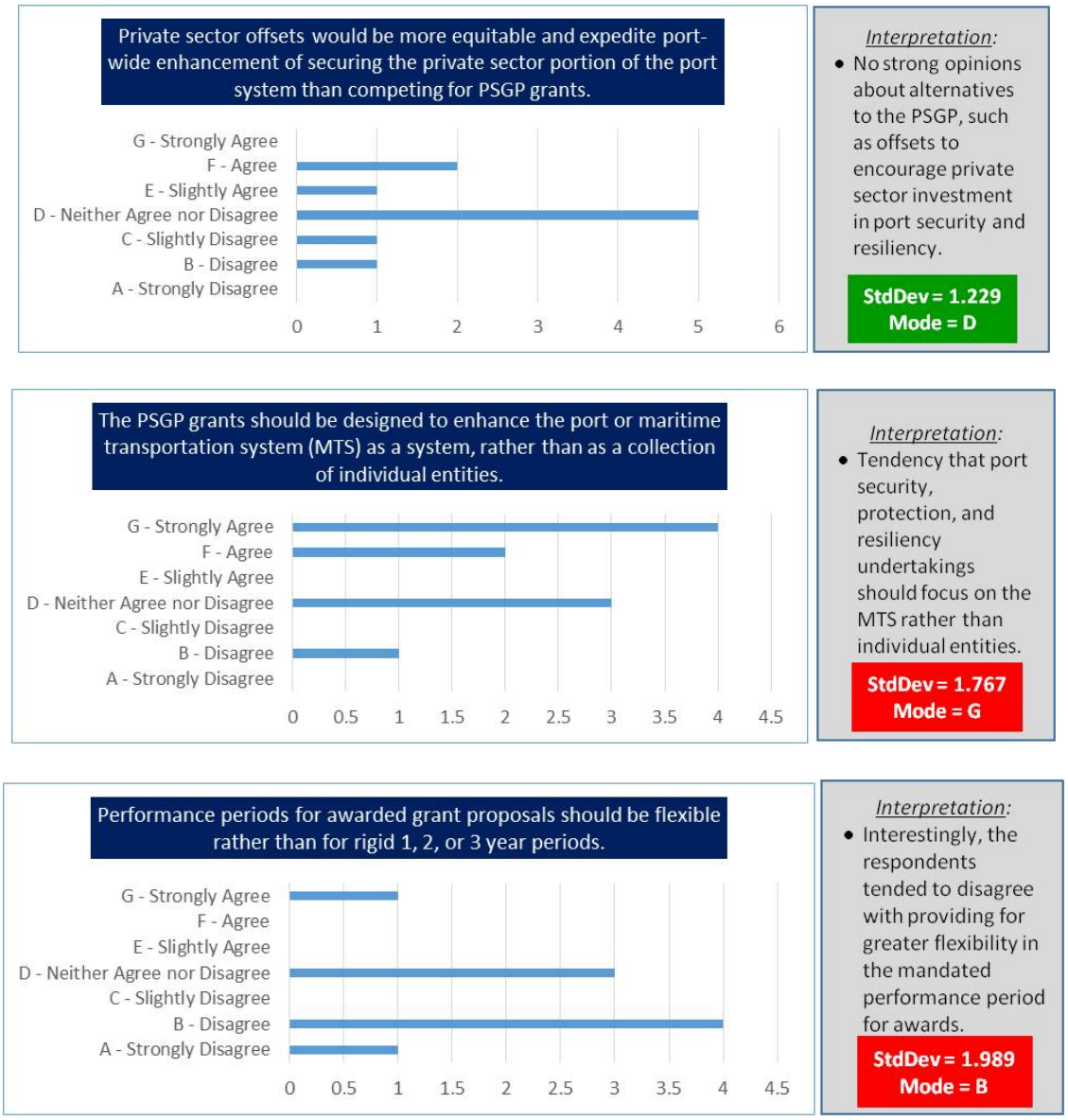


Figure 21. Survey Results.

Table 2. Survey Response Summary for the Remaining Questions.

What is your Area Maritime Security Committee's region?	Have you or your organization successfully competed for PSGP funds?	What type of PSGP stakeholder do you represent?	What historic Port Tier/Group was your port under the PSGP Tier/Group System?	Has your AMSC developed a Port-wide Risk Mitigation Plan (PRMP) &/or Business Continuity/Resumption of Trade Plan (BCRTP)?	Does your AMSC actively collaborate with other regional security working groups, such as UASI groups and Transit Security Working Groups?	If "Yes" to the last question, is the PRMP &/or BCRTP regularly reviewed and kept current/up-to-date?	Should the PSGP be focused on improving port PROTECTION, RESILIENCY, or BOTH?
AMSC - Sector Boston	Yes	H - Other	B - Tier 2	Yes	Yes	Yes	Both
AMSC - Sector Delaware Bay	Yes	H - Other	A - Tier 1	Yes	No	No	Both
AMSC - Sector Boston	No	A - Federal Agency	D - Other	Yes	Yes	No	Protection
AMSC - Sector Delaware Bay	No	F - Port Facility	B - Tier 2	Yes	No	Yes	Both
AMSC - Sector Delaware Bay	Yes	C - City/Local Agency	A - Tier 1	Yes	No	No	Both
Other	No	A - Federal Agency	B - Tier 2	Yes	No	No	Both
AMSC - Sector Boston	No	A - Federal Agency	B - Tier 2	Yes	Yes	Yes	Both
AMSC - Sector Boston	Yes	C - City/Local Agency	B - Tier 2	Yes	Yes	Yes	Both
AMSC - Sector Delaware Bay	Yes	H - Other	A - Tier 1	Yes	Yes	Yes	Both
AMSC - Sector Boston	No	H - Other	D - Other	No	No	Yes	Both

Table 3. All Survey Responses.

Have you or your organization successfully competed for PSGP funds?	Yes	Yes	No	No	Yes	No	No	Yes	Yes	No
What type of PSGP stakeholder do you represent?	Other	Other	Federal Agency	Port Facility	City/Local Agency	Federal Agency	Federal Agency	City/Local Agency	Other	Other
What historic Port Tier/Group was your port under the PSGP Tier/Group System?	Tier 2	Tier 1	Other	Tier 2	Tier 1	Tier 2	Tier 2	Tier 2	Tier 1	Other
The Port Security Grant Program (PSGP) Has Significantly Enhanced Port Security.	Agree	Agree	Slightly Agree	Agree	Strongly Agree	Slightly Agree	Agree	Strongly Disagree	Strongly Agree	Agree
Awarding of PSGP grants is closely tied to the Coast Guard MS-RAM analysis.	Strongly Disagree	Disagree	Agree	Agree	Strongly Agree	Disagree	Strongly Agree	Agree	Slightly Agree	Neither Agree nor Disagree
PSGP grants are closely aligned with risk-based Port Security Risk Assessments.	Slightly Disagree	Strongly Disagree	Slightly Agree	Agree	Strongly Agree	Disagree	Agree	Agree	Agree	Agree
The PSGP guidelines are closely aligned with meeting the goals of the National Maritime Security Strategy.	Slightly Disagree	Agree	Slightly Agree	Slightly Agree	Strongly Agree	Slightly Agree	Agree	Agree	Agree	Slightly Agree
Consolidation of the PSGP under an umbrella Homeland Security Grant Program would be good for continuing to enhance port security.	Neither Agree nor Disagree	Strongly Disagree	Strongly Disagree	Slightly Disagree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Strongly Disagree	Slightly Disagree
The disallowance of consortiums to compete for the PSGP has had a positive impact on improving port security.	Disagree	Strongly Disagree	Slightly Disagree	Slightly Disagree	Strongly Disagree	Disagree	Neither Agree nor Disagree	Neither Agree nor Disagree	Strongly Disagree	Neither Agree nor Disagree
Port Security could be better served if AMSCs could compete for PSGP grants to fulfill gaps in Area Maritime Security Assessments and their respective Area Maritime Security Plans instead of individual port stakeholders competing against one another.	Agree	Strongly Agree	Strongly Agree	Agree	Agree	Strongly Agree	Strongly Agree	Disagree	Slightly Agree	Agree
Other financial offsets could be as effective for promoting private sector investment in improved security, such as proportional tax deductions for security investments that meet the goals of the National Maritime Security Strategy.	Neither Agree nor Disagree	Slightly Agree	Strongly Agree	Slightly Disagree	Disagree	Slightly Agree	Agree	Disagree	Strongly Disagree	Slightly Agree
Private sector offsets would be more equitable and expedite port-wide enhancement of securing the private sector portion of the port system than competing for PSGP grants.	Neither Agree nor Disagree	Neither Agree nor Disagree	Agree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Disagree	Neither Agree nor Disagree	Neither Agree nor Disagree
The PSGP grants should be designed to enhance the port or maritime transportation system (MTS) as a system, rather than as a collection of individual entities.	Strongly Agree	Neither Agree nor Disagree	Agree	Neither Agree nor Disagree	Neither Agree nor Disagree	Strongly Agree	Strongly Agree	Disagree	Agree	Strongly Agree
Performance periods for awarded grant proposals should be flexible rather than for rigid 1, 2, or 3 year periods.	Disagree	Disagree	Neither Agree nor Disagree	Neither Agree nor Disagree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Disagree	Strongly Agree	
Has your AMSC developed a Portwide Risk Mitigation Plan (PRMP) &/or Business Continuity/Resumption of Trade Plan (BCRTP)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Does your AMSC actively collaborate with other regional security working groups, such as UASI groups and Transit Security Working Groups?	Yes	No	Yes	No	No	No	Yes	Yes	Yes	No
If "Yes" to the last question, is the PRMP &/or BCRTP regularly reviewed and kept current/up-to-date?	Yes	No	No	Yes	No	No	Yes	Yes	Yes	Yes
Should the PSGP be focused on improving port PROTECTION, RESILIENCY, or BOTH?	Both	Both	Protect	Both	Both	Both	Both	Both	Both	Both
	A - Strongly Disagree; B - Disagree; C - Slightly Disagree; D - Neither Agree nor Disagree; E - Slightly Agree; F - Agree; G - Strongly Agree									

C. FINDINGS FROM INTERVIEWS

1. The Coast Guard MS-RAM Program[165]

The Coast Guard's MS-RAM database continues to be relied upon to help inform PSGP proposal review. MS-RAM uses various attack scenarios to test critical infrastructure vulnerability to the specific threat vectors presented in the scenario. Based on the outcome of the scenario analysis, risk scores are determined. The Coast Guard provides these risk scores to FEMA for calculating an applicant's relative risk and the suitability of a PSGP proposal.

Time and again, the GAO recognizes the Coast Guard's progress on improving the MS-RAM, while noting that MS-RAM is not capable of calculating port-wide risk reduction or return on investment towards that end for executed PSGP proposals. MS-RAM is a hypothetical analytic tool; it cannot predict the probability of any particular attack mode, or even if it will be one of the modes pre-defined in the program, nor can it predict the degree of impact. All that it can provide is the potential success and an estimation of the degree of impact that a facility could realize if presented with a particular scenario.

2. PSGP Broadly[166]

The PSGP is a valuable resource for aiding ports in addressing port security concerns. The port security program under MTSA has matured over the past decade and a half incorporating lessons learned and establishing Area Maritime Security Committees (AMSC) and Port-Wide Risk Mitigation Plans (PRMP) as organizations and roadmaps, respectively, for achieving port security improvement. However, recurring challenges continue to daunt the PSGP. The following citations from a Coast Guard District's feedback are representative of recurring themes nationally:

---

165 Respondent 10688, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

166 Respondent 12987, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

- "The Port Security Grant program (PSGP) continues to demand an ever-increasing amount of time, attention, and oversight, placing an additional workload on the COTP and their staff for this unfunded mandate. Furthermore, the compressed and unrealistic timelines associated with the PSGP places considerable stress on the COTP and AMSC to schedule, facilitate, and complete the field review phase. Finally, the Coast Guard has become the face of the PSGP and applicants continue to direct application, award, and post-award questions to the COTP and their staff [rather than to FEMA GPD]."[167]

- "Cyber related vulnerabilities are a growing portion of the total risk exposure facing the Marine Transportation System (MTS), and it continues to be a challenge for COTPs, AMSCs, and maritime stakeholders. Aside from the requirement to report a cyber-attack (or potential attack) or breach of security that could lead to a Transportation Security Incident (TSI), there is no regulatory jurisdiction to require cyber security measures. Additionally, other than raising awareness through the AMSCs or creating cyber security related subcommittees, COTPs and their staffs have limited knowledge and training to support cyber security preparedness within their port areas."[168]

- And as the program has aged, "COTPs have noted decreasing AMSC membership throughout the District. Part of this is due to reduce operating budgets at other agencies and organizations, especially in COTP zones with expansive AORs. "[169]

Additionally, PSGP applicants consistently complained that they never receive feedback on why proposals fail to win grant funding. This simple act could significantly improve successful funding proposals. The vagaries of grant awards still swing dependent upon the quality of the grant writer as much as the worthiness of the proposal.

---

[167] Commander, Coast Guard Ninth District (CCGD9), Prevention Division (dp) letter 16600 dated April 3, 2015.

[168] CCGD9.

[169] CCGD9.

3. PSGP Specifically[170]

There is universal frustration from both the public and private sector port stakeholders outside Washington, D.C., with the perception that the national program managers dismiss the resident knowledge, experience, and expertise of the local AMSC stakeholders. AMSC members invest a great deal of time and effort to provide accurate and substantive input to the port assessments and the investment justifications for individual proposals. By the time they come under review at the national level, the input appears to be dismissed, with the final result seeming arbitrary.

At the most fundamental level, this is a case of poor communications and marketing by the national program managers. While local stakeholders acknowledged that they are not in a position to prioritize proposals and assessments across a national spectrum, they are confident in their knowledge of the regional MTS and their ability to assess the port's vulnerability. The absence of transparency in national level port evaluations undermines local stakeholders' confidence in the PSGP process.

It is demotivating when an AMSC's priority listing of risks, vulnerabilities, and criticality is apparently ignored and overridden by the national program without consultation or explanation with the AMSC. The general impression is that no one has a better understanding of the local concerns than the local stakeholders. The AMSC port stakeholders expressed frustration with revisions of port assessments and the vetting of proposals in an apparent vacuum or without local consultation that results in a sense of disenfranchisement.

It must be clear that this is not an indictment of the FEMA GDP or even its predecessor PSGP administrators. It may, in fact, be an artifact of the apparent disconnect between the PSGP Guidelines—focusing on individual entities rather than the MTS as a system—and overarching national level policies which identify

[170] Respondent 81950, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016; Respondent 36758, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016; Respondent 16258, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

the MTS as a system of systems requiring a systems approach to improving port security and resiliency. It may also be a function of FEMA's experience with grants administration; FEMA grants have historically addressed mitigating risk or damages to individuals and individual entities (even if the entities are a jurisdiction). That type of administrative philosophy predisposes responding to individual needs. What is needed is a philosophical shift to align program administration with national level policy and better process transparency and dialectic with the port stakeholders.

A consensus from respondents felt that the use of a fiduciary agent (FA) and submission of proposals by consortia should at the very least be an option. The forced "one size fits all" format in the latest iterations of the PSGP Notice of Financial Opportunities (NOFO) in some cases precludes taking advantage of the best possible option for improving the security and resiliency posture of a port by only accepting single-entity-only proposals. The FA, in the case of consortia and port-wide proposals, has in many cases served their port community well as an "honest broker" and "project manager." The FA has ensured that investment justifications (IJ) are well designed and actionable. The FA then maintains an oversight role ensuring that metrics and milestones are met. The allowance for consortia seems to be an obvious positive option. If we accept that the port is a system, in fact, a system-of-systems, then disallowing consortia runs contrary to that assessment. Consortia, by definition, are a collection of entities—a system.

While respondents believed that plan proposals from consortia should be allowed to compete, they also recognized the equal value in individual entities' competing for grant funding. There are instances where either option poses an opportunity to improve port security and resiliency.

However, FEMA is also constrained by the construct of the grant design, which would have to be modified to allow for the greater flexibility necessary to address many of these recommendations. FEMA's GDP staff of professionals have vast grant management and analytical experience. While consortia and fiduciary agents have been found to be beneficial options for some stakeholders,

individual direct funding has been so for other stakeholders and proposals. GDP also points out that the use of FA's comes at a cost, too.

First, a direct cost. FAs are compensated for their program oversight by attaching a surcharge to the grant disbursement; typically, 3% to 5% of the gross grant amount funded. The second is an indirect cost but has the potential to exacerbate the criticism about transparency and communications between stakeholders and program managers. With a fiduciary agent, FEMA GDP cannot communicate with the stakeholders directly, but must work through the fiduciary agent. It is up to the fiduciary agent to continue the communications down to the stakeholders. The prohibition on FEMA GDP's responding directly with grantees may have led to some of the stakeholder comments voicing frustration with an apparent lack of transparency and communications when in fact they should have addressed their questions through the FA. Direct communications between FEMA GPD and grantees is systemically obstructed when an FA is used. Either grant applicants will have to accept the trade-off or the precepts for administering the PSGP will have to be changed. However, the implications of using and FA and the moratorium on direct communications between FEMA GDP and grant applicants should be more clearly communicated.

According to FEMA GDP, there is not a ban on consortia. To clarify, FEMA GDP is constrained by only being able to award a grant to a single entity for accountability, but within a port groups can organize into de fact consortia to submit a joint proposal. The caveat is that the proposal must be submitted by a single entity who will be (a) accountable for the execution of the proposal, and (b) be the single point of contact for FEMA as the grantee of record. For cost-share obligations, the grant applicant would be responsible for proving availability of matching funds, but any distributed cost-share between the consortia partners would have to be negotiated in a separate agreement between the parties to the consortia. The grant awardee would act as a de facto fiduciary agent for the partners in the consortia. Recognition of the consortia is external to the PSGP

and FEMA GDP. From the program manager's point of view, the grant is awarded to a single entity.

The 2015 PSGP NOFO leveled the cost match to 25% for both public and private sector applicants. Investment in security and resiliency enhancements is an expense. In the absence of a disruption, it is essentially equivalent to insurance. Insurance from a business perspective is an expense. The higher the match requirement, the less inclined a stakeholder is in participating in the PSGP competition, with the resulting missed opportunity to address a vulnerability. When asked if a tax benefit would encourage independent investment in the absence of winning a grant, the general response was that the savings in tax benefits are insignificant and less likely to encourage independent investment.

Another frequent complaint is that grants appear to be awarded to those that write the best grant proposal, drafted as proposals that are sure to include all the essential keywords in the NOFO. But, a proposal that captures all the NOFO keywords does not equate to the highest priority proposal for a region. This observation links back to the prior frustration with the apparent discounting of the AMSC's and Captain of the Ports' prioritization of proposals for their region.

The NOFO suggests that proposals be linked to the existing Port-wide Risk Management Plan although the PRMP is no longer required and maintenance of the previously constructed plan is only a recommendation. Two issues come to light. The first is, the PRMP by design identifies a plan for improving port-wide security and resiliency. It provides a plan, with gaps analyzed, and a roadmap to closing those gaps. The PRMP provides a real metric for assessing the degree of risk reduction. A port-wide proposal should not just be allowed, but encouraged to address systemic risk.

The PSGP eliminated the port tier or port group system. All ports now compete in the same pool of PSGP funds so that there is no longer any specifically set-aside funding for different scale ports. The concern is that if DHS determines final prioritization of grant awards, the smaller ports will lose to the

mega-ports; that will leave untended backdoor opportunities for terrorist to take advantage. It is important to remember that 9–11 terrorist pilot Muhammed Atta's crew came through the small local Portland, ME airport on their way to Boston's Logan International Airport to avoid attention.[171] The smaller ports, remote from major metropolitan areas provide similar cover. The impression of the respondents was that the former port tier or group system ensured that some PSGP funding was distributed throughout the United States' MTS networks at all levels, and not just to the high visibility mega-ports.

One final observation regards port cyber-security, which is rapidly becoming a great national level concern. To date, national outreach efforts with the private sector have not been effective. Attendees at a recent port cyber-security events have been largely from various levels of government, academia, and think tanks; not the private sector (Recall that the majority of the MTS infrastructure is owned and operated by the private sector). Engagement has to be inclusive of all port stakeholders. Outreach will be critical. For proprietary reasons, the maritime industry is reticent to sharing information, as even providing the port destination for certain cargoes can significantly impact market values. The concern to protect proprietary commercial information is particularly true for those commodities sold on the spot market. Gaining stakeholder trust will be dependent upon convincing the private sector that proprietary information will be well protected.

Under the NIPP, many of the CI Sectors have ISACs—Information Sharing and Analysis Centers. There is a Maritime ISAC—the Maritime Security Council. The Maritime ISAC's "mission is to advance the security of the United States and the international maritime community by representing maritime interests before government bodies; acting as liaison between industry and government; disseminating timely information; encouraging and assisting in the development of industry-specific technologies; and convening educational and

[171] 911 Report, 306.

informational conferences for our membership and government partners."[172] While reference to the Maritime ISAC is absent in the PSGP, the ISAC could be leveraged to address much of the communication challenges MTS made by port stakeholders.

D. REPRESENTATIVE EXAMPLES—FAILURE FROM LACK OF RESILIENCY

Two recent products from the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) Office of Cyber and Infrastructure Analysis (OCIA) provide very clear illustrations of the need for elevating resiliency as an essential factor in managing risk to the MTS. The first report is a scenario-based analysis of the expected impacts of an extended and unanticipated closure of the Poe Lock, the major lock within the Soo Locks joining Lake Superior to Lake Huron via the St. Mary's River past the twin cities of Sault Ste. Marie, MI, USA and Sault Ste. Marie, ON, Canada. The second report is an analysis of the potential consequences of a cyber-attack on the MTS.

1. OCIA Analysis of Poe Lock Disruption

The DHS made public the OCIA's October 2015 report on "*The Perils of Efficiency: An Analysis of an Unexpected Closure of the Poe Lock and its Impact*." While the vast majority of ports are a tangled web of interdependent multi-sector nodes, the Great Lakes steel industry is very homogeneous and, therefore, provides a very succinct example of the consequences of interdependency.

The Soo Locks are a series of locks built, maintained, and operated by the U.S. Army Corps of Engineers. Currently, only two locks are operating within the Soo Locks: The Poe Lock and the MacArthur Lock. Of the two, only the Poe Lock is capable of locking through the dominate Great Lakes Thousand Footers—Great Lakes ships purpose-built to operate on the Great Lakes

[172] The Maritime Security Council, http://www.maritimesecurity.org/, 2015 (accessed March 11, 2016).

transporting bulk product, largely taconite ore and coal, for the steel industry. The U.S. fleet never leaves the Great Lakes. The MacArthur Lock is unable to accommodate the Thousand Footers, and can only lock through substantially smaller vessels. The two other locks in the U.S. portion of the system are currently decommissioned—the Davis and Sabin Locks—unserviceable and too shallow to lock through the existing fleet of Lakers. The one lock on the Canadian side is only capable of serving recreational boating traffic.[173] Figure 22 is a satellite photograph captured from Google Earth of the Soo Locks with essential landmarks labeled.

Figure 22. Screenshot from Google Earth accessed 06 March 2016.

The OCIA based the scenario on a hypothetical unscheduled six-month closure of the Poe Lock during the primary shipping season, from March 25th to

[173] Personal knowledge as Coast Guard Ninth District Prevention Division Chief responsible for the Coast Guard's Waterways Management mission in the U.S. Great Lakes system.

September 25th.'[174] The study focused on impacts to the supply chains serviced by vessels transiting the Soo Locks.

The economic impact from the cascading effects of the unscheduled closure of the Poe Lock for the six prime shipping months would have a devastating effect across sectors of the economy, and internationally to a major extent in Canada and Mexico.[175] The report is extensive and highly detailed, summarized significantly herein for illustrative purposes.

Iron ore is mined primarily in the western Lake Superior basin of Minnesota and North Dakota.[176] The ports of Duluth, Two Harbors, and Silver Bay in Minnesota and Superior, Wisconsin are the four loading ports for taconite.[177] The destination ports are all in Lake Michigan and Lake Erie, through the Soo Locks.

The scenario generated closure of 74 percent of the U.S. steel production; in particular, those mills that the appliances, automobile, construction, farming, mining equipment, and rail car manufacturing industries are substantially dependent.[178] The automotive industry would eventually have to shutter, as it would be impossible to source the specific grades of production steels cost effectively from non-U.S. mills. According to the Analysis, over 50 distinct

---

[174] Navigation on the Great Lakes is seasonal, between freezing over of the Lakes (a moving target itself) and the closure of the Soo Locks and the Welland Lock (that by-passes Niagara Falls allowing "salties," or ocean-going vessels, to transit to and from the Great Lakes and the ocean.) After the locks close (the "closed season"), domestic U.S. and Canadian shipping continues until ice conditions become prohibitive; U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *The Perils of Efficiency: An analysis of an Unexpected Closure of the Poe Lock and its Impact*, (Washington, DC: Homeland Security Information Network, 2015), 19.

[175] OCIA, *The Perils of Efficiency*, 25.

[176] There is one mine in the northern part of Michigan's Upper Peninsula, which ships ore by trains to the ports of Marquette on Lake Superior, and Escanaba on Lake Michigan in Green Bay which is converted into taconite pellets for transport. Escanaba is the only shipping port for taconite not in Lake Superior. (OCIA, *The Perils of Efficiency,* 20).

[177] It is noteworthy that there are many grades of taconite pellets and they are not interchangeable, but are specific to a particular type of steel being produced from them. (OCIA, pp. 2–3).

[178] OCIA, *The Perils of Efficiency,* 20.

industries identified by unique North American Industrial Classification System (NAICS) codes would be severely impacted with service impacts of 20 to 100 percent.[179]

The six-month closure of the Poe Lock translates in economic terms to a 10-month shutdown of the automobile industry—production and sales, along with all of the just-in-time suppliers either without a customer to sell to, or themselves knocked out of production. The national economy would realize losses of $1.1 trillion in GDP—a 6 percent decrease[180]—and over 10 million jobs.[181] The unemployment rate is estimated to jump an additional 5.8 percent; more than doubling the current rate that is hovering around 5 percent,[182] with the model projecting "10.9 million people out of work in the United States, with additional losses in Canada and Mexico."[183]

The OCIA study provides the following contextual contribution of a single Laker[184] trip:

- A Thousand Footer[185] carries approximately 70,000 short tons of taconite.
- The cargo value (in current dollars U.S.) is approximately $4 million.
- The four-year average of iron ore shipped through the Poe Lock is 46.2 million tons annually.
- Each ton of ore generates $23,000 of economic value.

---

179 OCIA, *The Perils of Efficiency,* Appdx. E.

180 OCIA, *The Perils of Efficiency,* 34.

181 Ibid., 20.

182 Ibid., 30.

183 Ibid., 32.

184 A purpose-built commercial ship that only works upon the Great Lakes.

185 A large Great Lakes carrier, generally around 1000' in length. Capable of transiting only through the Poe Lock.

- Each Laker shipment represents $1.7 billion in U.S. economic business, and an estimated contribution of $340 million to the Canadian and Mexican economies.[186]

The industries that rely upon the steel made from Great Lakes iron ore (taconite) have realized a great economic benefit from the efficiencies gained by transporting taconite from the ore fields via Great Lakes carriers, through the Soo Locks. The entirety of their profitability is dependent upon the reliable, timely, and cost-effective delivery of taconite by Laker. The industry built around the Great Lakes MTS. In fact, the mills are laid out only to receive ore from the waterside, with rail and over-road service, if any, for outbound product shipment. Neither the railroads nor over road trucking can replace the Lakers service.[187]

Even if the facilities were designed to be able to accept ore from rail or truck, neither would be capable of meeting the demand—alone or in conjunction. Furthermore, if the capability existed, they are cost prohibitive options. Ancillary to the economic impossibilities is the fact that, by wide margins, neither rail shipment nor trucking is as safe or ecologically-friendly as the Lakers.[188] The infrastructure to supplant the Lakers by rail or road does not exist. But, if it did, it would take approximately 2000 railcars added to an already congested Midwestern rail system.[189]

Moving taconite by truck is more dramatic. "Each One Thousand Footer Lake Carrier carries approximately 70,000 tons of iron ore, which is equivalent to about 3,000 trucks. The mills use the 70,000 tons about every five days, which means that 600 trucks per day—1 truck every 2.4 minutes—would have to enter a steel mill, drop its load and leave. To bring trucks to 7 mills would mean that, for every point on the Interstate Highway System between Minnesota and Indiana, there would be a truck loaded with iron ore passing every 20 seconds on

---

186 OCIA, *The Perils of Efficiency,* 34.

187 OCIA, *The Perils of Efficiency,* 41–45.

188 Ibid., 41–45.

189 Ibid., 43.

one side of the road and one truck returning empty on the other side of the road. The Interstate Highway System would have to be shut down to all traffic except for the iron ore trucks and no road maintenance could occur."[190]

Notably, the Poe Lock is a single point of failure potential of monumental proportions. The report goes on to cite potential mitigation options and then proves them untenable. The best option for mitigating the dependency on the Poe Lock is to build a second Poe Lock. The problem there is that it would be next to the existing Poe Lock. Assuming the loss of the lock is due to attack or massive scale natural or man-made disaster, then whatever impacts the current lock would undoubtedly do so to the other. An additional Poe Lock adds resiliency by way of redundancy, and only as protection against certain scenarios.[191]

The complexity of the MTS in most ports is greater than the Poe Lock scenario. However, in that networked system of systems, virtually all of which grew as an emergent system that evolved over time, is an opportunity for building resiliencies. There may very well already be prospects to cultivate resiliency within the natural ecosystem of the port MTS system of systems that are not currently recognized.

2. OCIA Analysis: Consequences to Seaport Operations from Malicious Cyber Activity

On March 3, 2016, the DHS/NPPD/OCIA issued a paper entitled "Consequences to Seaport Operations from Malicious Cyber Activity." The report focuses on the cyber vulnerabilities presented by the dependency on information systems to efficiently manage the complex MTS. As a system of systems, the

---

[190] OCIA, *The Perils of Efficiency,* 45.

[191] Ibid., 52. (An important point is that, if a second Poe Lock were to be built, it would have to be the exact same dimensions as the current Poe Lock. If a larger capacity lock were built, larger ships would be built to take advantage of the economies of scale, returning us back to the same single point of failure scenario we face now.)

MTS is reliant upon other sectors as other sectors are dependent upon the MTS.[192] Examples of sectors interdependent with the MTS are:

The MTS is dependent upon the following Sectors—

- Energy
- Water & Wastewater
- Emergency Services
- Communications
- Financial Services
- Government Facilities
- Transportation
- Information Technology

The Sectors Most Dependent upon the MTS are the following—

- Energy
- Food and Agriculture
- Transportation
- Critical Manufacturing
- Chemical
- Commercial Facilities
- Transportation
- Defense Industrial Base[193]

The report cites the tremendous reliance of all aspects of the MTS on information technology to function. That dependency breeds susceptibility to many modes of failure, from specific targeted attacks to human error to technology obsolescence and inability to interface with other systems. Information technology helps navigate ships; track cargo; manage cargo handling, shipping, and warehousing operations; control access and security; Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems; and transaction handling—and this is a far from an all-inclusive list.[194] Couple IT systems with cellular service, GPS-enabled/

[192] U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, Consequences to Seaport Operations from Malicious Cyber Activity, (Washington, DC, Homeland Security Information Network, 2016), 1–2.

[193] Not cited in OCIA, Consequences to Seaport Operations.

[194] OCIA, Consequences to Seaport Operations, 3–16.

dependent services, Wi-Fi wireless networking, telemetric systems, web-based programs, and there suddenly are many gateway opportunities to exploit.

A vivid example of how vulnerable GPS is to spoofing—GPS spoofing is the use of a signal that is stronger than and mimics the attributes of a genuine GPS signal to take over a GPS receiver. The ability to send a signal that could cause the vessel's GPS receiver to report a position chosen by the attacker that is somewhere other than where the receiver actually is[195] was demonstrated by University of Texas at Austin students off the coast of Italy.

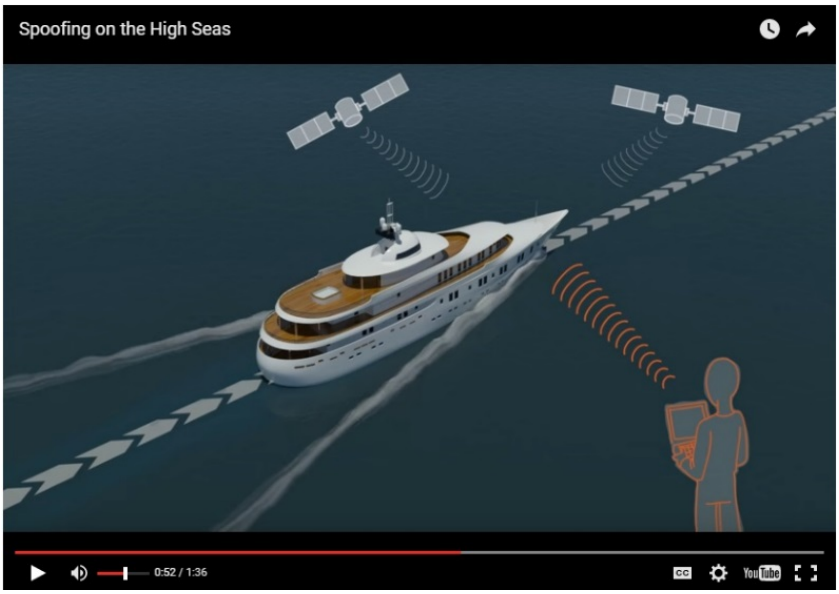


Figure 23. Screenshot from University of Texas at Austin, Cockrell School of Engineering, *UT Austin Researchers Spoof Superyacht at Sea*, Monday, Jul 29, 2013, http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.

The UT students successfully spoofed the GPS signal being received by the 213' super yacht M/V WHITE ROSE, replacing the legitimate GPS signal with a false one generated by their custom-made device, with the vessel's crew completely oblivious to the attack.

[195] The IT Law Wiki at http://itlaw.wikia.com/wiki/GPS_spoofing accessed March 8, 2016.

The previous year the same University of Texas team successfully hijacked an unmanned aerial vehicle (UAV) by intercepting its GPS signal and replacing it with a spoofed signal, taking over control of the UAV. The UT team, of course, are "white hats," attempting to raise awareness of the vulnerability posed by GPS dependency. They argue "[w]ith 90 percent of the world's freight moving across the seas and a great deal of the world's human transportation going across the skies, we have to gain a better understanding of the broader implications of GPS spoofing," Professor Humphreys said. "I didn't know, until we performed this experiment, just how possible it is to spoof a marine vessel and how difficult it is to detect this attack."[196]

Unquestionably, cyber-security is a critical aspect of the MTS infrastructure that must be protected and made more resilient. The span of cyber-security concerns reaches beyond any single entity within the MTS; it is the network that weaves throughout the MTS and connects the MTS to the other Sectors. Information technology and communications (cyber) is the nervous system of the complex system of systems that is the MTS.

3. Transfer of PSGP HLS Boat[197]

One of the persistent challenges champions of the PSGP face are the stories of waste and mismanagement—sometimes real, sometimes perceived—that Secretary Chertoff mentioned in his 2007 press conference remarks on the Fiscal Year 2007 Infrastructure Protection Grants Program.[198] There are many such stories about assets purchased with capabilities that far exceed the capacity of the grantee to operate, manage, and maintain or stories about equipment purchased placed in storage, never used for HLS missions. However,

---

[196] UT News, Cockrell School of Engineering, University of Texas, July 30, 2013, http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea accessed March 8, 2016.

[197] Recounted from personal experience as the Coast Guard Fifth District Northern Region Director of Auxiliary, Philadelphia, PA from June 2013 to June 2015.

[198] U.S. Department of Homeland Security, "*Remarks by Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2007 Infrastructure Protection Grants Program,"* January 09, 2007, 4–5.

the vast majority of grants were executed in fulfillment of the winning proposal. The important question is not "Were the grant funds used to fulfill the grant proposal?," but rather "Did funding the grant proposal diminish risk?"

One more story: The Borough of Marcus Hook, Pennsylvania competed for and won a 2004 PSGP grant to purchase a $202,000.00 SAFE Boat configured for law enforcement/homeland security patrols along the city's Delaware River boundary. The Borough of Marcus Hook, Pennsylvania is home to Sun Oil, multiple refineries, the Commodore Barry Bridge to New Jersey, spider-webbed with rail and pipelines, Marcus Hook ship anchorage, and bounded by the Delaware River to the east and Interstate 95 to the west. The Borough of Marcus Hook is a worthy hub of critical infrastructure to protect.

By 2010 the Marcus Hook police officers that were trained to operate the vessel had retired or left the Marcus Hook Police Department. The Borough soon realized that ownership and operation of such a high-performance vessel was an expensive commitment. Crews had to be trained to handle the vessel, and constantly train and exercise in operating it to maintain competency. Insurance, fuel, storage, maintenance costs are very expensive challenges as well. The Borough decided it would be best to try and divest itself of the SAFE Boat.

Conveniently, the Coast Guard Auxiliary[199]—a wholly voluntary civilian organization affiliated with the U.S. Coast Guard—was interested in accepting the donation of the Marcus Hook SAFE Boat. There was a concern about the potential conflict of interest in accepting the SAFE Boat since the U.S. Coast Guard cannot benefit directly from PSGP grants. With the legal determination made that, though the CG Auxiliary is related to the U.S. Coast Guard, it is not part of the Coast Guard per se and was, therefore, eligible to receive the gifted SAFE Boat. FEMA, as the PSGP administrator, was requested to provide a legal

[199] The U.S. Coast Guard Auxiliary is an all-volunteer civilian cadre whose mission is to assist the Coast Guard in promoting recreational boating safety, augment the Coast Guard and enhance safety and security of our ports, waterways, and coastal regions, and to support Coast Guard operational, administrative, and logistical requirements. (From http://cgaux.org/about.php accessed February 20, 2016).

determination on the disposition of the SAFE Boat's transfer to the CG Auxiliary. (Figure 24)

The response from FEMA was "Because Grant #2004-EU-T3-0041 is closed, FEMA does not retain a financial interest in the disposition of the SAFE Boat. After a grant closes, all jurisdictions that purchased equipment with Homeland Security Grant Funds should follow their policies and procedures for disposition of surveyed or excess equipment."

U.S. Department of Homeland Security
Washington, DC 20472

FEMA

Mark P. Much, Esquire
341 West Baltimore Avenue
Media, PA 19063

Re: FEMA Grant # 2004-EU-T3-0041.

Dear Mr. Much,

In 2005, the Borough of Marcus Hook Police Department, Pennsylvania was provided with Office of Domestic funds under Grant # 2004-EU-T3-0041. These funds were used to purchase a SAFE Boat at a cost of $202,000.00. I understand that the Borough Law Enforcement Officers who were trained to use the boat have retired or left the force and the Borough can no longer afford to utilize this asset.

I understand that the Borough is in the process of entering into a licensing agreement with Division 4, 5th District Northern Region, United States Coast Guard Auxiliary ("Auxiliary") which will provide the Auxiliary with an exclusive license to a building located on the Delaware River with deep water dockage. This building will be used as a training station and to further the Auxiliary's mission to contribute to the safety and security of coastal regions. I understand that the Borough is seeking approval from FEMA to transfer ownership of the SAFE boat to the Auxiliary.

Because Grant #2004-EU-T3-0041 is closed, FEMA does not retain a financial interest with the disposition of the SAFE Boat. After a grant has been closed, all jurisdictions that purchased equipment with Homeland Security Grant Funds should follow their policies and procedures for disposition of surveyed or excess equipment. The Borough of Marcus Hook may transfer the Safe Boat to the United States Coast Guard Auxiliary; however they must retain records of the transfer for a minimum of 3 years. I have attached the final Grant Adjustment Notice which states Grant #2004-EU-T3-0041 was closed on January 10, 2010.

Sincerely,

Dennis Donehoo
Program Analyst, Grant Programs Directorate

CC: Grant File
Southeastern Pennsylvania Regional Task Force
Pennsylvania Emergency Management Agency

Figure 24. FEMA letter regarding disposition of Homeland Security SAFE Boat.

Nothing is suggested to be out of order in the disposition of the SAFE Boat transfer to the Coast Guard Auxiliary. However, there certainly are questions that can be—and should be—raised about accountability of grant recipients' ability to responsibly manage assets purchased through PSGP grant proposals, how effective any given proposal can be expected to improve the security of the MTS, and the appropriateness of a proposal for MTS security. A reasonable observer could perceive that the transfer of the SAFE Boat to the Coast Guard Auxiliary was a waste of almost one-quarter million dollars of taxpayer money.

E. INTERPRETATION, ANALYSIS, FUSION AND SYNTHESIS OF ALL RELEVANT DATA AND EVIDENCE

The PSGP was initially intended to provide public sector port entities with funding to support hardening of the port infrastructure from terrorist attack. Examples of port hardening include installation of closed circuit cameras, purchase of watercraft and vehicles for patrolling the ports, and to ensure interoperability between jurisdictions and agencies. Future iterations of the PSGP evolved to include port security funding to the private sector MTS stakeholders as well, but, still they were focused on hardening the infrastructure.

Protection, as mentioned earlier, is defensive by nature, and as such, is a "brittle strategy."[200] Program managers recognized that and began including port resiliency as doctrine.

However, apparent contradictions in PSGP guidelines prove problematic to achieving resiliency as a PSGP target goal. Some examples of apparent contradictions include:

- Applicants are "encouraged" to submit proposals consistent with the AMSC's Area Maritime Security Plan. But they don't have to.
- Proposals should support filling gaps in the respective AMSC's Port-Wide Risk Mitigation Plans (PRMP). But the PRMP is optional, and its maintenance not required—although encouraged.

[200] CRS R42683, 2012, 13 and Summary.

The MTS is a system of systems,[201] yet the current PSGP guidance disallows consortia—a system of stakeholders—from submitting coordinated systems-oriented proposals. The PSGP only allows for proposals from individual entities rather than coordinated proposals from interdependent port stakeholders that focus on the port system.

[201] DHS, "National Strategy for Maritime Security–Maritime Transportation System Security Recommendations," 2.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS

The frustrations and inefficiencies recognized by the port stakeholders have been called out in a previous thesis published at the Center for Homeland Defense and Security. Pamela N. (Broughton) Haverkos noted in her March 2009 thesis on "Measuring Preparedness: Assessing the Impact of the Homeland Security Grant Program," that "[t]he lack of a common preparedness vision … and the time compressed requirements have all contributed to the inability to measure the impact the HSGP has made on preparedness."[202] Seven years later, the Port Security Grant Program continues to suffer from the same issues that the greater HSGP has had to struggle with, without resolution.

The PSGP had flirted with good policy, but then changed direction. Throughout this research, the PSGP was found to fill a very tangible need but is doing so in a less than optimal fashion. The recommendations that follow are not in any particular order, but rather are all considered important opportunities to improve the PSGP.

A. MAINTAIN THE PSGP AS A DISCRETE GRANT PROGRAM

First and foremost, it is recommended that the Port Security Grant Program remain a separate and specific grant program rather than becoming incorporated into a broad, universal Homeland Security Grant Program. Because the ports are part of our national borders and through which over 90% of our international trade takes place, the PSGP must remain a standalone grant program.

B. IMPROVE TRANSPARENCY OF PROPOSAL REVIEW AND GRANT AWARD PROCESS

One of the criticisms from the field that has dogged the PSGP throughout its existence is the lack of transparency in the proposal vetting process and

[202] Pamela N. Broughton, "Measuring Preparedness: Assessing the Impact of the Homeland Security Grant Program" (master's thesis, Naval Postgraduate School, 2009), 67.

absence of good and timely feedback to AMSCs on why proposals were accepted or not. This lack of good communication throughout the PSGP cycle has led to a sense of disenfranchisement by the very community being asked to work towards improving the security and resiliency of its port system.

The national level program needs to incorporate into the PSGP process a 360º feedback loop. Currently, FEMA GPD hosts pre-announcement conferences, in person and by teleconference, in advance of the NOFO's release. However, after that, very little contact is made with the applicant communities. The following communications processes are recommended:

- GPD should provide periodic progress updates.
- GPD's outreach effort should always be ongoing. The development of the PSGP guidelines needs to be a perpetually iterative process that fully engages all constituents.
- Engage the Maritime Security Council as a national information hub for port security. The Maritime Security Council is the Transportation Sector's Maritime Subsector Information Sharing and Analysis Centers (ISAC).

C. JETTISON THE COOKIE CUTTER

1. Allow the Employment of Fiduciary Agents and Consortia as an Option

The PSGP on occasions has provided alternative avenues to problem solving. The use of fiduciary agents (FA) and allowance for consortia to submit proposals are two examples. Use of both the fiduciary agent and explicit allowance for consortia are no longer options. The tendency of the PSGP guidelines has been to publish a "one size fits all" process where the same constraints apply to all applicants, or all applicants within a port category. Addressing port security by a cookie cutter template is suboptimal. The adage of "if you have seen one port, you have seen one port" is accurate. Some are mega-ports with an eclectic mix of commercial activity operating throughout the MTS, situated in major metropolitan areas and part of an intermodal hub. Other

ports are small, specialized areas far from major population centers. All are ports of entry. A one-size-fits-all model will not work with such diversity.

For some project proposals, a fiduciary agent may be the best process for achieving a proposal goal. Since ports are systems, and systems within other systems, to address port security and resiliency ONLY by addressing individual entities is inadequate to addressing the risks of disruptions to ports. Consortia, on the other hand, are a well suited option for addressing shared systemic port security and resiliency shortfalls across multiple entities.

Due to the variety of port types and the infinite number of risks and challenges faced by the nation's diverse ports, the best way to assure the highest return on investment from grant awards is by allowing the greatest flexibility to achieving the goal of the PSGP. Accountability is a critical capability for any public program. The PSGP has had challenges in accounting for how much any given grant award has reduced risk.

The decision to allow for the use of fiduciary agents and consortia is not the best process for every proposal. There are the additional costs to consider, such as the FA's surcharge (of on average 3%–5% of the grant value) and inability for grantees to have direct communications with FEMA GPD. These are tradeoffs to consider when planning a project proposal for a grant award under the PSGP.

Metrics are critical for efficient project management. A quick way to establish good PSGP metrics is to require each port to maintain an up to date port-wide risk mitigation plan (PRMP) with grant proposals linked to closing a specific PRMP gap, and then evaluate how well the proposal succeeded in filling that gap and reducing risk. The scale then becomes a relative measure of success at reducing the risk posed by the identified gap in a given port's PRMP.

2. Not all Ports are the Same

The PSGP struggled with and modified a port tier or group process across many versions. At times there were up to four different tiers or groups,[203] down to three, then two, now none. During the tier/group variants of the PSGP, a certain pool of funding was set aside for each tier. Members of each tier/group competed against each other for the pool allotted to their contingent. Understandably, this system weighted priority to provide a greater pool of funding to those ports that represented a higher risk to the nation if disrupted.

With all ports competing against one another, the likelihood is that the historic Tier/Group I ports will have greater success at competing for PSGP funds than the lesser ports. As evidenced by the earlier example of how hijacker Atta managed to avoid notice by flying into Boston from Portland, ME, smaller ports matter. The tier/group system assured all ports could compete for limited resources, allocated by the relative risk and consequence for the given port.[204]

Early in the PSGP, specific funding levels were pre-identified for specific ports. The first grant awards were direct grants to ports of predesignated amounts. Table 4 details the initial allocations of port security grants in the Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program:[205]

---

[203] The name changed from tier to group over the course of time, but the mean the same thing.

[204] Respondent 16258, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

[205] Department of Homeland Security, "The Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program," http://ojp.gov/archives/solicitations/docs/fy03uasi_psg.pdf. (accessed January 10, 2016).

FISCAL YEAR 2003 UASI PORT SECURITY GRANT PROGRAM FUNDING ALLOCATIONS			
Port / Amount		**Port / Amount**	
New York/New Jersey	$9,371,21	Los Angeles/Long Beach	$9,076
Seattle	$6,765,72	Hampton Roads	$6,600
Miami	$6,595,00	Houston	$6,546
Philadelphia	$6,450,21	New Orleans	$6,400
Beaumont	$5,611,56	Charleston	$5,124
Port Canaveral, FL	$4,352,37	San Juan, PR	$1,605
Valdez	$250,00	LA LOOP	$250
TOTAL: $75,000,000			

Table 4. Initial Allocations of Port Security Grants. Source: The Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program.

FEMA observed that ports put minimal effort into grant spending proposals when they were guaranteed a certain amount of funding.[206] Alternatively, when all ports compete against one another without weighting or set-asides, the smaller—but no less potential target—ports are at risk of losing out to the larger ports for grant funding.

A better solution would be a blending of the two approaches for deciding funding amounts, whereby grouping ports would again use risk and consequence potential with a guaranteed set-aside pool for each group to compete for. Port grouping with funding set-asides had been used in the 2007 PSGP Guidelines and was generally appreciated by grant applicant stakeholders. 2007 was when the program moved from a list of pre-identified eligible ports to grouping ports into tiers based on some factors including the variables in the risk equation. Each Tier would receive a block of funding to compete for funding proposals. The Fiscal Year 2007 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit allocated grant fund by tiered port in Table 5:[207]

[206] Respondent 16258, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

[207] Department of Homeland Security, *Fiscal Year 2007 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*, 5, http://www.fema.gov/pdf/government/grant/psgp/fy07_psgp_guidance.pdf. (accessed January 7, 2016).

PSGP FY07 Available Funding ($ millions)	
• Tier I:	$120,702,000
• Tier II:	$40,234,000
• Tier III:	$30,175,500
• Tier IV:	$10,058,500
TOTAL $201,170,000	

Table 5. Allocated Grant Fund by Tiered Port. Source: Fiscal Year 2007 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit.

It is recommended that the PSGP restore allocation of funds through the port tier or group prioritization practice, as was done for FY 2007.

3. Require AMSC's to maintain the PRMP/ BCRTP

It is highly recommended that all ports develop and maintain a Port-wide Risk Management Plan (PRMP) and Business Continuity/Resumption of Trade Plan (BCRTP). A well-developed and maintained PRMP and BCRTP provides for clearly articulated consensus on a security and resiliency plan for a given AMSC's port system. The PRMP/BCRTP provides a means for measuring the degree of risk reduced by awarded grant funds, as well as suggesting clear ways forward for successive grant cycles.

Done properly, the PRMP/BCRTP is a roadmap to continual improvement for the port's security and resiliency posture, informing successive iterations, and a living feedback loop to the AMSC and program managers in Washington, DC. By having a port-wide, long-term plan with clearly established performance milestones, DHS and FEMA will be able to articulate to Congress exactly where the money has gone and how it has improved port security and resiliency. Furthermore, the PRMP/BCRTP process, by design, approaches port security and resiliency from the perspective of systems management. They fully align with the National Preparedness Goal.

As such, a PRMP/BCRTP MTS-wide strategy would benefit from an allowance for consortiums to form and submit proposals and compete equally with all port stakeholders for PSGP awards.

4. Cost Sharing; Less is More for the Private Sector[208]

The legislation requires a 25% cost share. Prior NOFOs had split cost share percentages between the public and private sector (i.e., 25% for public sector entities and 50% for private sector entities), perceived by the private sector as an intentional effort to drive funding towards the public sector. Without a mandate beyond the minimal requirements under the MTSA, the private sector viewed additional investment in security and resiliency as costs that subtracted from the bottom-line without any guaranteed return on investment. There is insurance for business disruptions, but insurance is discretionary spending. A disruptive event could come from any number of directions, the least of which was probably from the waterside of the facility. Less likely even yet would be a terrorist attack. Private sector participation may increase if the cost-share percentage becomes a flat 25% for both the public and private sectors.

It is recommended that the cost share percentage remain at the minimum 25% for both public and private sector entities.

5. Core Capabilities as PSGP Objectives Must Be Revised

The PSGP consistently insists that proposals be designed to address the core capabilities from the National Preparedness Goal. Those core capabilities are:

(1) Strengthening governance integration;

(2) Enhancing strategic ports within the National Port Readiness Network;

(3) Enhancing Maritime Domain Awareness (MDA);

[208] Respondent 12563, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

(4) Enhancing Improvised Explosive Device (IED) and Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) prevention, protection, response and supporting recovery capabilities within the maritime domain;

(5) Enhancing cybersecurity;

(6) Maritime security risk mitigation projects that support port resilience and recovery capabilities, as identified in an Area Maritime Security Plan or facility security plan;

(7) Training and exercises; and

(8) Transportation Worker Identification Credential (TWIC) Implementation.[209]

Item (1) is profoundly vague. However, it should stay that way for maximum flexibility. Improvement of governance is always good.

Item (2) is certainly a national priority, but not necessarily one of the highest in importance to regional private sector port stakeholders. This is a federal priority and should be a direct line item for federal expenditure, not an additional burden on the local economy or private sector port stakeholders.

Item (3), MDA, has been a struggle that has not been fully realized. Done properly, MDA would be provided by a blending of federal, state, and local intelligence sharing with a liaison to the private sector, perhaps through the Maritime ISAC.

Item (4) is defense oriented, and as previously highlighted, is a brittle strategy. If, as by the National Preparedness Strategy, the goal is to be prepared for "all hazards," this legacy of early post-911 reaction is too narrowly focused and should be re-written to speak broadly of including resiliency measures versus solely defensive ones.

Item (5) is a nascent apprehension that is gaining momentum, as we realize that digitizing has made us more vulnerable to attack. The greater

[209] Port Security Grant Program (PSGP) - Grants Office LLC, http://www.grantsoffice.com/GrantDetails.aspx?gid=17040 (accessed April 06, 2016).

efficiencies we have realized through digital technologies have also made us more dependent, interdependent, and vulnerable.[210]

Cyber security is a valid and important aspect of port security, and it deserves to be supported to the full extent of enabling capability, to include the PSGP.

Item (6) speaks to AMSPs and port resiliency and recovery capabilities. Those capabilities recognize the MTS as an interdependent system of systems, not separate entities.

To fulfill this requirement, the PSGP must allow consortia to participate in the grant competition along with individual entities to support holistic port-wide port security and resiliency plans.

Item (7) is important and figures strongly in the development of those relationships and realization of the depth of interdependency that exists within the MTS. Training and exercises are an essential function for building port security and resiliency and should continue to be encouraged.

Item (8), Transportation Workers Identification Credential, has long since deployed. TWIC should be removed as a specific line-item capability from the PSGP. All MTSA regulated entities required now to comply with the TWIC regulations.

6. Re-visit the Risk Equation

The Risk Equation is ubiquitous. It has become so commonplace that it is often assumed to be a fundamental truth that is seldom challenged or questioned. It is recited by muscle memory and even accepted as a mathematical fact by non-mathematicians, on comparable footing with the Pythagorean Theorem or Einstein's $E=mc^2$. But it is not a mathematical formula;

[210] Unrestricted first-person knowledge experienced during my tour in DHS, National Protection and Program Directorate, Office of Infrastructure Protection.

it is a model that attempts to simplify relationships between variables that influence Risk.[211] Instead of

$$\boldsymbol{R}isk = \boldsymbol{V}ulnerability \times \boldsymbol{T}hreat \times \boldsymbol{C}onsequence$$

a better model is

$$\boldsymbol{R = f[(V)(T)(C)]}.$$

That is, Risk is a Function of the relationships between Vulnerability, Threat, and Consequence. The PSGP's early focus on defensive measures addressed changing the ***V****ulnerability* variable of the equation. By building resiliency into port systems, the PSGP seeks to modify the ***C****onsequence* variable. The ***T****hreat* variable is best controllable through intelligence to provide opportunities for disrupting intentional threats through preemptive measures. It is more difficult to modify the Threat variable for natural events, as they are primarily geographically determined, and a certain degree of prediction and probability is possible.

The Coast Guard's MS-RAM program uses this latter variant of the Risk Equation, adding weighting factors to each variable, to estimate the ***R****isk* of a specific asset in a given scenario. However, we must be careful not to fall into the trap that the number generated is related to any mathematical solution. It does not equate to any greater or lesser probability that something will happen.[212]

---

[211] Jeff Lowder, August 23, 2010 post on BloInfoSec.com, http://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/ (accessed January 19, 2016).

[212] Respondent 10668 and 13563, Interview by Paul Arnett, telephone, Cleveland, March 9, 2016.

VI. CONCLUSION

> *"The German thrust into Western Europe in World War II is a natural analog: The Wehrmacht simply side-stepped the impressive defenses built by the French in the Maginot Line. Similarly, terrorists will attack wherever the defenses are weakest."*[213]

Ms. Rugy's statement directly relates to the Port Security Grant Program (PSGP), as the focus has been from the start on hardening critical infrastructure (CI) through direct funding of individual entities rather than looking at the port as a system. By focusing on the brittle strategy of defensive measures versus reinforcing the resilience of the MTS, the PSGP is largely in the business of building Maginot Lines, or worse, building independent pill boxes, which the *Threat* can bypass rather than directly confront. This analogy applies to natural and man-made disruptive events.

Instead, the goal of the PSGP should be to make the MTS like a block of ballistic gel; able to absorb impact and still retain its shape.

The national level policy makes strengthening, maintenance, protection, and building resiliency into, our critical infrastructure a national priority. To the point, PPD-21 states:

> Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure–including assets, networks, and systems–that are vital to public confidence and the Nation's safety, prosperity, and well-being.
>
> The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space

[213] Veronique de Rugy, "What Does Homeland Security Spending Buy?," "What Does Homeland Security Spending Buy?," *AEI Economic Policy Working Paper Series* (2005): 5.

> and cyberspace, and governance constructs that involve multilevel authorities, responsibilities, and regulations.[214]

Critical infrastructure is recognized by national policy as a complex system of interdependent systems. Yet, after a decade and a half, the PSGP still focuses on individual entities within a port system rather than require proposals that address broader MTS security and resiliency shortfalls. The NIPP speaks of "cascading effects"[215]—the dropping dominos of second, third, and tertiary order critical infrastructure impacts from events. It is within the cascade that the greatest costs of an event are realized.

Our nation has built its economic vitality on the efficiencies gained from leveraging proximity, networked synergies, digitization, and just-in-time deliveries. These technologies and strategies are great for business, provided there are no threats to that system of systems. Unfortunately, al-Qaida and its ilk have stated their intentions are to bring down America by destroying the U.S. economy.

What made the U.S. economy so effective and competitive also makes it vulnerable. With over 90% of U.S. trade occurring through the seaports, the MTS represents a very attractive target. Terrorists can exploit two different attack modes through the MTS: a direct attack on the port itself, or use the MTS as a gateway for moving persons and materiel into the U.S. to support operations elsewhere within the U.S.

The ports are the final line of defense before terrorists enter the country. They are an essential node of the economy. They are fundamentally open to facilitate commercial activity. The general population seldom notices the seaport as they drive past them.

Located on the water, the MTS is highly vulnerable to not only terrorist attack but natural disasters. Hurricanes, flooding, ice jams, failed levees, storm

---

[214] *Presidential Directive / PPD-21*—Critical Infrastructure Security and Resilience, 1.

[215] DHS, NIPP 2013.

surge, climate change all have severely impacted the MTS periodically. With a large number of process facilities located on the waterways, depending on the waterway for process water as well as for transportation, the potential for impact of the MTS from accidental man-made source has a long history as well.

The MTS deserves specific, targeted federal support to improve its security and resiliency posture. Doing so should be a national priority. The PSGP is an excellent vehicle for doing so. It has, on occasion, exhibited promising insight and potential to affect improvement in the status quo of port security and resiliency. And at times, it has backed away.

The PSGP must remain a program dedicated to improving the status quo of port security and resiliency. The MTS is a system of systems. With that recognition, PRMPs should be used as both proposal justification as well as the means to measure efficacy. It must accept port-specific proposals, to include accepting consortia and if suitable, fiduciary agents to facilitate proposal execution, as well as from individual port stakeholders. The one-size-fits-all cookie cutter model is unacceptable and inefficient. Such an approach guarantees each and every GAO report for the out years will include the phrase "FEMA is making progress but …."

The PSGP must maintain a discrete port-centric homeland security grant program. The cost-share obligation must remain 25% for both public and private sector grantees. Reestablishing the tier group port system with set-asides for each tier/group will ensure all ports have a fair chance to win priority, proportional funds.

The Port Security Grant Program, indeed, can be made better.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

American Association of Port Authorities. "*The 2014 National Economic Impact of the U.S. Coastal Port System."* Martin Associates (Lancaster, PA, 2015).

———. *"U.S. Public Port Facts."* last modified 2013. http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032.

Bouchard, Joseph F., Ph.D. "*New Strategies to Protect America: Safer Ports for a More Secure Economy*." Center for American Progress. Washington, D.C., 2005.

Broughton, Pamela N. "*Measuring Preparedness: Assessing the Impact of the Homeland Security Grant Program*." Master's thesis, Naval Postgraduate School, 2009.

Cavallo, Antonella. "*Integrating disaster preparedness and resilience: a complex approach using System of Systems*." Refereed Article, PhD candidate at the University of Adelaide, 2014.

Commander, Coast Guard Ninth District (CCGD9), Prevention Division (dp) letter 16600 dated April 3, 2015.

Clovis, Samuel H. Jr. "*Promises Unfulfilled: The Sub-Optimization of Homeland Security National Preparedness*." Homeland Security Affairs, v. IV, no. 3, October 2008.

Colvin, Catherine V. "*DHS Homeland Security Grant Program: The Influence of Committee Membership on Grant Allocations for FYs 2004–2006*." Master's thesis, Georgetown University, 2007.

Congressional Research Service. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress,* by Todd Masse, Siobhan O'Neil, and John Rollins. CRS RL33858, 2007 (accessed November 15, 2015 at http://fas.org/sgp/crs/homesec/RL33858.pdf).

Congressional Research Service. *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, by John D. Moteff. CRS R42683, 2012, (accessed January 6, 2016 at http://fas.org/sgp/crs/homesec/R42683.pdf).

DeLaurentis, D., and Callaway, R. K. "*A System-of-Systems Perspective for Public Policy Decisions*." (2004), Review of Policy Research, 21: 829–837. doi:10.1111/j.1541-1338.2004.00111.x.

de Rugy, Veronique. "*What Does Homeland Security Spending Buy?*" *AEI Economic Policy Working Paper Series* (2005).

Department of Homeland Security. *American Recovery and Reinvestment Act of 2009, Port Security Grant Program Guidance and Application Kit*, May 2009, http://www.fema.gov/pdf/government/grant/arra/fy09_arra_psgp_guidance.pdf (accessed January 7, 2016).

———. *Fiscal Year 2003 Urban Areas Security Initiative Port Security Grant Program*. http://ojp.gov/archives/solicitations/docs/fy03uasi_psg.pdf. (accessed January 10, 2016).

———. *Fiscal Year 2005 Port Security Grant Program (PSGP): Program Guidelines and Application Kit*. https://www.fema.gov/pdf/government/grant/psgp/fy05_psgp_guidance.pdf . (accessed January 7, 2016).

———. *Maritime Transportation Security Act of 2002 Press Kit*: *Protecting America's Ports*. Washington, DC. July 2003.

———. *National Infrastructure Protection Plan (NIPP).* Washington, DC. 2013.

———. *National Infrastructure Protection Plan 2013*. Washington, DC. https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf . (accessed January 30, 2016).

———. *National Infrastructure Protection Plan 2013 Transportation Sector Specific Plan*. Washington, DC. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (accessed January 30, 2016).

———. *National Strategy for Maritime Security: The Maritime Infrastructure Recovery Plan 2006*. Washington, DC.

———. *National Strategy for Maritime Security–Maritime Transportation System Security Recommendations*. Washington, DC. https://www.dhs.gov/xlibrary/assets/HSPD_MTSSPlan.pdf. (accessed January 30, 2016).

———. *Notice of Funding Opportunity Fiscal Year 2015 Port Security Grant Program (PSGP)*. Washington, DC. http://www.fema.gov/media-library-data/1429282564066-3b452acb7dc7a2f1460a15ed855547d9/FY2015PSGP_NOFO_v2.pdf. (accessed January 7, 2016).

———. *Fiscal Year 2006 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. https://www.fema.gov/pdf/government/grant/psgp/fy06_psgp_guidance.pdf . (accessed January 7, 2016).

———. *Fiscal Year 2007 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. http://www.fema.gov/pdf/government/grant/psgp/fy07_psgp_guidance.pdf. (accessed January 7, 2016).

———. *Fiscal Year 2008 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. http://www.fema.gov/pdf/government/grant/psgp/fy08_psgp_guidance.pdf . (accessed January 7, 2016).

———. *Fiscal Year 2009 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. http://www.fema.gov/pdf/government/grant/psgp/fy09_psgp_guidance.pdf . (accessed January 7, 2016).

———. *Fiscal Year 2010 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. https://www.fema.gov/pdf/government/grant/2010/fy10_psgp_guidance.pdf . (accessed January 7, 2016).

———. *Fiscal Year 2011 Infrastructure Protection Program: Port Security, Program Guidelines and Application Kit*. Washington, DC. https://www.fema.gov/pdf/government/grant/2011/fy11_psgp_kit.pdf. (accessed January 7, 2016).

———. *Fiscal Year 2012 Port Security Grant Program (PSGP) Funding Opportunity Announcement (FOA)*. Washington, DC. https://www.fema.gov/pdf/government/grant/2012/fy12_psgp_foa.pdf. (accessed January 7, 2016).

———. *Fiscal Year 2013 Port Security Grant Program (PSGP) Funding Opportunity Announcement (FOA)*. Washington, DC. http://www.fema.gov/media-library-data/20130726-1916-25045-9099/fy13_psgp_foa_final.pdf. (accessed January 7, 2016).

———. *Funding Opportunity Announcement (FOA) Fiscal Year 2014 Port Security Grant Program (PSGP)*. Washington, DC. http://www.fema.gov/media-library-data/1396623742630-9e497a99bef3e3c0265bbf84993b5e69/FY_2014_PSGP_FOA_Final_Revised.pdf. (accessed January 7, 2016).

———. *Notice of Funding Opportunity (NOFO) Fiscal Year 2015 Port Security Grant Program (PSGP)*. Washington, DC. http://www.fema.gov/media-library-data/1429282564066-3b452acb7dc7a2f1460a15ed855547d9/FY2015PSGP_NOFO_v2.pdf. (accessed January 7, 2016).

———. *Notice of Funding Opportunity (NOFO) Fiscal Year 2016 Port Security Grant Program (PSGP)*. Washington, DC. http://www.fema.gov/media-library-data/1455573875236-07ce03a778118ecc2ead8e1aae84185e/FY_2016_PSGP_NOFO_FINAL.pdf. (accessed January 7, 2016).

———. Overview: FY 2007 Infrastructure Protection Program. Washington, DC. January 2007.

———. (*The 2014) Quadrennial Homeland Security Review,* Washington, DC. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf, June 2014. (accessed February 14, 2016).

———. *Remarks by Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2007 Infrastructure Protection Grants Program. Washington, DC.* January 09, 2007.

———. Review of the Port Security Grant Program (OIG-05-10). Washington, DC. January 2005.

———. *What's New in the National Response Framework*. Washington, DC. http://www.fema.gov/pdf/emergency/nrf/whatsnew.pdf, January 22, 2008. (accessed December 10, 2015).

———. Written testimony of [DHS Office of] POLICY, USCG, CBP, TSA, FEMA for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Evaluating Port Security: Progress Made and Challenges Ahead." Washington, DC. June 4, 2014.

Electronic Code of Federal Regulations, *Title 33: Navigation and Navigable Waters, Part 101 Maritime Security: General, Subpart B-Maritime Security (MARSEC) Levels, 101.200 MARSEC Levels*, http://www.ecfr.gov/cgi-bin/text-idx?SID=06484778d56042f2ad2adb178235c8df&mc=true&node=se33.1.101_1200&rgn=div8 (accessed January 07, 2016).

Electronic Code of Federal Regulations, *Title 33: Navigation and Navigable Waters, Part 101 Maritime Security: General, Subpart C-General, Records Retention, and Enforcement, 101.105 Definitions*, http://www.ecfr.gov/cgi-bin/text-idx?SID=06484778d56042f2ad2adb178235c8df&mc=true&node=se33.1.101_1105&rgn=div8 (accessed January 07, 2016).

Federal Emergency Management Administration. *NPG Core Capabilities*. FEMA.gov. http://www.fema.gov/core-capabilities (accessed December 10, 2015).

Flynn, Steven. *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism.* New York: Harper Collins in cooperation with the Council on Foreign Relations, 2004.

———. *America the Resilient Defying Terrorism and Mitigating Natural Disasters*. *Foreign Affairs* (2008), http://www.nyu.edu/intercep/lapietra/Flynn_AmericatheResilient.pdf, accessed January 9, 2016.

———. *The Edge of Disaster: Rebuilding A Resilient Nation.* New York: Random House in cooperation with the Council on Foreign Relations, 2007.

Government Accountability Office. *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*, GAO-06-618 Washington, D.C., 2012. http://www.gao.gov/new.items/d06618.pdf (accessed January 6, 2016).

———. *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*. GAO-12-14. Washington, DC. November 2011.

———. *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs.* GAO-12-303. Washington, DC. February 2012.

———. *Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress, Statement of William O. Jenkins, Jr., Director Homeland Security and Justice*, GAO-12-526T. Washington, D.C., 2012. http://www.gao.gov/assets/590/589446.pdf (accessed January 6, 2016).

———. *Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response*, GAO-12-494R. Washington, D.C., 2012. http://www.gao.gov/assets/590/589946.pdf (accessed January 6, 2016).

———. *Maritime Security: Progress and Challenges with Selected Port Security Programs, Statement of Stephen L. Caldwell, Director, Homeland Security and Justice*. GAO-14-636T. Washington, D.C., 2012. http://www.gao.gov/assets/670/663784.pdf (accessed January 6, 2016).

———. *National Preparedness: FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities, Statement of David C. Maurer, Director Homeland Security and Justice*. GAO-13-637T. Washington, D.C., 2012. 5. http://www.gao.gov/assets/660/655392.pdf (accessed January 6, 2016).

———. *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*. GAO-12-47. Washington, D.C., 2012. http://gao.gov/assets/590/587142.pdf (accessed January 6, 2016).

———. *Recovery Act: FEMA Could Take Steps to Protect Sensitive Port Security Grant Details and Improve Recipient Reporting Instructions*. GAO-11-88. Washington, DC. October 2010.

———. *Testimony Before the Subcommittee on Emergency Management, Intergovernmental Relations, and the District of Columbia, Committee on Homeland Security and Government Affairs, U.S. Senate. National Preparedness: FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities*. GAO-13-637T. Washington, DC. June 2013.

———. *Testimony before the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, House of Representatives. National Preparedness: FEMA Has Made Progress in Improving Grant Management and Assessing Capabilities, but Challenges Remain*. GAO-13-456T. Washington, DC. March 2013.

Haimes,Yacov, Joost Santos, Kenneth Crowther, Matthew Henry, Chenyang Lian and Zhenyu Yan. "Chapter 21: Risk Analysis in Interdependent Infrastructures." *Risk Analysis*, v.32, No.11. New York. (2012).

Haimes, Yacov Y., Kenneth Crowther, Barry M. Horowitz. "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems." Center for Risk Management of Engineering Systems, University of Virginia. Published online 16 June 2008 in Wiley InterScience: DOI 10.1002/sys.20101.

Himber, Lisa B. "Policymaking in the Port Security Grant Program: A look at the effectiveness of the decision to discontinue the use of the Fiduciary Agent model." Master's paper, Drexel University. Philadelphia, PA. 2015.

Homeland Security Act of 2002, 6 U.S.C.§101. Washington, DC. (2002).

Homeland Security Advisory Council: Report of the Critical Infrastructure Task Force. https://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf. January 2006. (accessed February 10, 2016).

House Committee on Homeland Security. *The SAFE Port Act Fact Sheet*. Washington, DC. March 2006.

House, Committee on Homeland Security: Subcommittee on Border, Maritime, and Global Counterterrorism. *The Safe Port Act: A Six-Month Review*, Hearing, April 26, 2007 (Serial No. 110–31). Washington: Government Printing Office, 2007.

Hubbard, Douglas W. *The Failure of Risk Management: Why It's Broken and How to Fix It.* New Jersey: John Wiley and Sons, 2009.

IT Law Wiki at http://itlaw.wikia.com/wiki/GPS_spoofing accessed March 8, 2016.

Kimmance, James Peter, and Anthony John Harris. "Infrastructure Risk and Resilience: A Review." *The Institution of Engineering and Technology*. Hertfordshire, UK. 2013.

Mansouri, Mo, and Alex Gorod, Thomas H. Wakeman, Brian Sauser. "A Systems Approach to Governance in Maritime Transportation System of Systems." School of Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ. 2009.

Maritime Administration. *2011 U.S. Water Transportation Statistical Snapshot. November 2013*. Washington, DC. http://www.marad.dot.gov/wp-content/uploads/pdf/US_Water_Transportation_Statistical_snapshot.pdf, (accessed October 2, 2014).

Maritime Security Council, website http://www.maritimesecurity.org/, 2015, accessed March 11, 2016.

Monier, Jerry T., Jr. “Clarifying Resilience in the Context of Homeland Security.” Master’s thesis, Naval Postgraduate School. Monterey, CA. 2013.

National Security Presidential Directive - NSPD-41/Homeland Security Presidential Directive HSPD-13— Maritime Security Policy (Washington, D.C.: The White House, 2004). http://fas.org/irp/offdocs/nspd/nspd41.pdf, (accessed January 30, 2016).

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.

National Infrastructure Advisory Council (NIAC), Critical Infrastructure Resilience Final Report and Recommendations. Washington, DC. September 8, 2009.

Office of Cyber and Infrastructure Analysis. *The Perils of Efficiency: An analysis of an Unexpected Closure of the Poe Lock and its Impact*. Washington, D.C., Homeland Security Information Network. 2015.

———. *Consequences to Seaport Operations from Malicious Cyber Activity*, Washington, D.C., Homeland Security Information Network. 2016.

Peters, Josh. *Overview of the United States Coast Guard’s Cyber Strategy and the MTS*. Presentation to Ninth Coast Guard District staff. Cleveland, OH March 29, 2016.

Port Security Grant Program (PSGP) - Grants Office LLC, http://www.grantsoffice.com/GrantDetails.aspx?gid=17040 (accessed April 06, 2016).

Presidential Policy Directive / PPD-21 (Washington, D.C.: The White House, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, (accessed January 9, 2016).

Presidential Policy Directive / PPD-8—National Preparedness (Washington, D.C.: The White House, 2011), https://www.dhs.gov/presidential-policy-directive-8-national-preparedness, (accessed October 11, 2015).

Senate Committee on Homeland Security and Governmental Affairs, *Evaluating Port Security: Progress Made and Challenges Ahead*, Hearing, Washington, DC. June 4, 2014.

USA Patriot Act of 2001, 42 U.S.C. 5195(e). U.S. Government Printing Office. Washington, DC. 2001.

U.S. Coast Guard. "U.S. Coast Guard, Missions, Maritime Security." Last Modified September 5, 2014. http://www.uscg.mil/top/missions/MaritimeSecurity.asp. (accessed November 02, 2014).

———. *"*U.S. Coast Guard, Ports, Waterways & Coastal Security (PWCS)*."* last modified January 12, 2016. http://www.uscg.mil/hq/cg5/cg532/pwcs.asp. (accessed November 02, 2014).

———. "Navigation and Inspection Circular 04–02: Security for passenger vessels and passenger terminals." Washington, DC. 2002.

———. "Navigation and Inspection Circular 09–02: Guidelines for development of area maritime security committees and area maritime security plans required for U.S. Ports.." Washington, DC. 2002.

———. "Navigation and Inspection Circular 10–02: Security guidelines for vessels." Washington, DC. 2002.

———. "Navigation and Inspection Circular 11–02: Recommended security guidelines for facilities." Washington, DC. 2002.

———. "Navigation and Inspection Circular 03–03: Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities." Washington, DC. 2003.

———. "Navigation and Inspection Circular 04–03: Guidance for verification of vessel security plans on domestic vessels by the regulations mandated by the Maritime Transportation Security Act (MTSA) Regulations and International Ship & Port Facility Security (ISPS) code." Washington, DC. 2003.

———. "Navigation and Inspection Circular 05–03: Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 for Outer Continental Shelf Facilities." Washington, DC. 2003.

———. "Navigation and Inspection Circular 10–04: Guidelines for Handling of Sensitive Security Information (SSI), parts 1 and 2." Washington, DC. 2004.

———. “Navigation and Inspection Circular 12–04: Maritime security compliance and enforcement for the U.S./Canadian boundary and coastal waters.” Washington, DC. 2004.

———. “Navigation and Inspection Circular 02–05: International Port Security (ISP) Program.” Washington, DC. 2005.

———. “Navigation and Inspection Circular 03–07: Guidance for the implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector.” Washington, DC. 2007.

———. “Navigation and Inspection Circular 01–13: Inspection and Certification of Vessels Under the Maritime Security Program (MSP).” Washington, DC. 2013.

University of Texas News, Cockrell School of Engineering, July 30, 2013, http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea accessed March 8, 2016.

Wikipedia contributors, “List of Countries by Length of Coastline,” *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=List_of_countries_by_length_of_coastline&oldid=692497936 (accessed January 10, 2016).

World Shipping Council. *“Trade Statistics.”* last modified 2014. http://www.worldshipping.org/about-the-industry/global-trade/trade-statistics

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California