2016

Business And Security In The Age Of Terrorism: The Long-Term Effects Of The September 11 Terrorist Attacks On Seaport Governance And Control

Daniel J. Ostergaard
University of South Carolina

BUSINESS AND SECURITY IN THE AGE OF TERRORISM: THE LONG-TERM EFFECTS OF THE SEPTEMBER 11 TERRORIST ATTACKS ON SEAPORT GOVERNANCE AND CONTROL

by

Daniel J. Ostergaard

Bachelor of Science
United States Coast Guard Academy, 1994

Master of National Security and Strategic Studies
United States Naval War College, 2003

Master of Public Administration
Harvard University, 2004

Submitted in Partial Fulfillment of the Requirements

For the Degree of Doctor of Philosophy in

Business Administration

Darla Moore School of Business

University of South Carolina

2016

Accepted by:

Andrew Spicer, Major Professor

Kendall Roth, Committee Member

Robert Rolfe, Committee Member

Richard Davis, Committee Member

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

DEDICATION

For Sarah, my true companion…

For Jack, William and Katie… that you may know the value of education and a life fully lived.

And for all those USCG, TSA and CBP members, law enforcement and first responders who have stood on the front lines of this newfound threat; who know the toil and terror and yet, don their uniform in the faith that their actions will bring about a better tomorrow for all mankind.

Sometimes I ask to sneak a closer look

Skip to the final chapter of the book

And then maybe steer us clear from some of the pain it took

To get us where we are this far…

But the question drowns in its futility

Even I have got to laugh at me

No one gets to miss the storm of what will be

Just holding on for the ride…

But the wood is tired, and the wood is old

And we'll make it fine, if the weather holds

But if the weather holds, we'll have missed the point

That's where I need to go…

-Emily Sailers, Excerpts from "The Wood Song"

ACKNOWLEDGEMENTS

If I have seen a little further it is by standing on the shoulders of Giants.
-Sir Isaac Newton, 1676

Words cannot convey the gratitude that I owe to so many. The first acknowledgement must be to the 4 people I love so dearly. Sarah (s.y.w.p.), Jack (wawa), William (pdivite) and Katie (triggle). Thank you for believing, for your patience and your sacrifice while I wrote. Kids who barely know a time when their father was *not* working on his doctorate.

Next, thank you to Jim, Nancy, Linda, Julie, Greg, David and Tina and especially, Mike. To John, Mabel, and Dorothy. To Aunt Sherrie for instilling within me a love of reading a long, long time ago. Thank you all for being integral to who I am.

To my USC family. Andy who was with me every single step of this journey. Kendall, Rob, Gerry, Angel, Kurt, Alex, Nick, Tolga, Hye Sun, Helen, Sabrina, Meike, AK, Babs, Matthias and especially BETH! What a voyage it has been… from the laughs to the tears you've been fine shipmates. I would not be here if not for you. Thank you!

To the WNC/WCU team for showing me how to grow, live and teach. To my Harvardianis homo sapiens & Sue: 525,600 minutes… how do you measure time? To the Potomac crew: Elections, "strategeries" and strategical… 753 Tenth - Toga. To the Coasties: A love of the sea and its lore: 65', 82', 140', 210', 295', 378', AOF-c, G-I.

As Winston Churchill penned, "*It is not the end, nor is this the beginning of the end, but it is, perhaps, the end of the beginning*."

ABSTRACT

The primary research goal of this dissertation is to improve our theoretical understanding of the long-term effects of major transnational terrorist events on security-related institutional changes for business. To accomplish this goal, the September, 11, 2001, terror attack was chosen as the starting point for this research. The research context is the governance of seaport security. Using grounded theory to develop comparative case studies of several major security initiatives in the maritime industry after 9/11, this dissertation shows that a terrorist event initiates a process of institutional change that emerges over time as initial security-related ideas cascade into concrete actions. In terms of seaport security, this research demonstrates that not only did the rules of the game changed as a result of a fear of future terrorist attacks but that both the actors and the governance structures changed as well. However, the changes that occurred cannot be easily inferred from reading the policies written soon after 9/11 that hoped to redesign institutional arrangements to better protect seaports from terrorist attacks. Instead, substantive change has slowly emerged over time from the complex negotiation between security, political and economic actors over the proper responsibilities of who implements and pays for desired security-related changes. Based on this analysis, I propose that exploring the effects of terrorism on business requires looking at the intersection of economic and security logics as institutional responsibilities are debated and redrawn in the face of an increasingly risky global business environment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAPA ..... American Association of Port Authorities

ACC ..... American Chemistry Council

AMSC ..... Area Maritime Security Committee

AMSP ..... Area Maritime Security Plan

ATA ..... American Trucking Association

AWO ..... American Waterway Operators

CBP ..... U.S. Customs and Border Protection

CBRN ..... Chemical, Biological, Radiological, and Nuclear

CBRNE ..... Chemical, Biological, Radiological, Nuclear, and Explosive

CFIUS ..... Committee on Foreign Investment in the United States

CI/KR ..... Critical Infrastructure/Key Resource

CIP ..... Critical Infrastructure Protection

COTP ..... Captain of the Port

COTP ..... Captains of the Port

CSI ..... Container Security Initiative

DAS ..... Deputy Assistant Secretary

DHS ..... U.S. Department of Homeland Security

DNDO ..... Domestic Nuclear Detection Office

DOD ..... U.S. Department of Defense

DOE ..... U.S. Department of Energy

DOT ..... U.S. Department of Transportation

DPW ..... Dubai Ports World

EMS ..... Emergency Medical Service

EOC..... Emergency Operations Center

EOP .....Emergency Operations Plan

FBI .....Federal Bureau of Investigation

FDI ..... Foreign Direct Investment

FEMA .....Federal Emergency Management Agency

FRP .....Federal Response Plan

FSP..... Facility Security Plans

GAO.....Government Accountability Office

GMCOI ..... Global Maritime Community of Interest

GSC-IAB..... Government Smart Card-Interagency Advisory Board

HSAC.....Homeland Security Advisory Council

HSPD .....Homeland Security Presidential Directive

IBT ..... International Brotherhood of Teamsters

IRB..... Institutional Review Board

ISAC .....Information Sharing and Analysis Center

JTTF.....Joint Terrorism Task Force

MARAD..... Maritime Administration

MARSEC ..... Maritime Security

Massport..... Massachusetts Port Authority

MDA ..... Maritime Domain Awareness

MRA .....Mutual Response Agreement

MSRAM.....Maritime Security Risk Analysis Model

MTSA .....Maritime Transportation Security Act of 2002

NIMS.....National Incident Management System

NIPP..... National Infrastructure Protection Plan

NISSC .....National Information Systems Security Conference

NIST.....National Institute of Standards and Technology

NMSAC .....National Maritime Security Advisory Committee

NPG..... National Preparedness Guidance

NRP..... National Response Plan

NSHS .....National Strategy for Homeland Security

NSMS.....National Strategy for Maritime Security

NSTS.....National Strategy for Transportation Security

OIG ..... Office of Inspector General

OMB .....Office of Management and Budget

P&O ..... Peninsular and Oriental Steam Navigation Company

PANYNJ .....Port Authority of New York and New Jersey

PCCIP ..... President's Commission on Critical Infrastructure Protection

PDD-63 ..... Presidential Decision Directive/NSC-63

PG&E.....Pacific Gas & Electric

PPD .....Presidential Policy Directive

PRMP.....Portwide Risk Mitigation Plan

PSGP ..... Port Security Grant

PSGP .....Port Security Grant Program

PSRAT .....Port Security Risk Assessment Tool

RAD/NUC..... Radiological/Nuclear

SAFE Port Act .....Security and Accountability for Every Port Act of 2006

SCPA.....South Carolina Ports Authority

SEPP .....Security Emergency Preparedness Plan

TEW.....Terrorism Early Warning

TIA.....Terrorism Incident Annex

TISD..... Transportation Infrastructure Security Division

TSA ..... Transportation Security Administration

TSGP ..... Transit Security Grant Program

TSI ..... Transportation Security Incident

TSOC ..... Transportation Security Operations Center

TWIC ..... Transportation Worker Identification Credential

UASI ..... Urban Area Security Initiative

UAWG ..... Urban Area Working Group

USCG ..... U.S. Coast Guard

USGC ..... United States Coast Guard

VTS ..... Vessel Traffic System

WMD ..... Weapons of Mass Destruction

INTRODUCTION AND OVERVIEW

"Businesses have to be resilient no matter what happens. If there is an event, a catastrophe or if there is a 9/11 type event, businesses have to able to get up and running quickly. And I think the architecture, whatever that is, needs to help create conditions to do that, and then get out of the way. I think as tragic as these events are, business is business. To be resilient, they have to get back on their feet and serve the public… It has been a decade of trying to learn how to do it. Crime and tragedies are nothing new… the difference with 9/11 was it was a catastrophic event that suspended day to day living. That had never happened before, at least not in my lifetime. There was a whole generation trying to figure out what it means to be resilient. I don't know if we are there yet. As a framework, I don't know if I see hard evidence that we are there. It's probably just the kind of thing that is just evolving. Maybe the answer is there is no framework. Maybe it has to be very decentralized - where the government just sort of plugs and plays where it can support different sectors and then help them get on their feet. What are you going to do? You can't give sectors money. The government doesn't have a lot of manpower and resources to give them. Probably what it can do is communicate with them and try to help with regulations and new laws if needed." – Comments from a senior government security official during an interview for this dissertation (Interview 11, 2016).

Existing security-related research in the field of business primarily takes a firm-level view on managing relatively well-known security concerns, thus looking at issues such as political risk and legitimacy at the level of a single firm (*e.g.*, Czinkota, Knight, Liesch & Steen, 2010). Yet, as evidenced by the scope of the impact that such punctuated terrorism-initiated events as 9/11 demonstrate, these events extend beyond a single firm to encompass change in the *underlying* rules of the game that define the institutional context of business. More importantly, transnational terrorist events often transform the security-related rules of business but also lead to the emergence of new types of security agencies and actors designed to monitor and enforce those rules in

practice. As the opening quotation illustrates, this debate over what those rules should be, and who should monitor, enforce and pay for security-related institutional changes in the private sector, represents a critical long-term effect of terrorism on the institutional environment of business.

In this dissertation, I propose that the most significant effects of a major transnational terrorist event are therefore likely to manifest themselves by initiating a process of institutional change and contestation, as politicians, security agents and economic actors come to question and revise the role of security goals and logics within existing political and economic systems. A major terrorism event is likely to initiate periods of institutional change when issues of national and organizational security move from the background of economic and political activity to its foreground, particularly as potential vulnerabilities are assessed and potential solutions are proposed.

To apply an institutional change perspective to the study of the intersection of business and security, I first build on institutional logics literature. Institutional logics are defined as sets of material practices and symbolic constructions that constitute societies' organizing principles (Friedland & Alford, 1987). While the literature has defined six ideal logics (family, religion, state, market, profession, and corporation), one contribution of my research is to introduce a seventh ideal type: security logic. In my theory chapter, I introduce the idea of an ideal security logic and how it relates to related concepts in the institutional logics literature.

I then explore the concept of an ideal security logic to anchor a discussion of the effects of major terrorist events on processes of institutional change over time. In contrast

to studies that delve into *ideal types* in isolation from other institutional logics, my research design considers the effects of logics hybridization and blending on processes of long-term institutional change. From this perspective, long-term institutional change is not the result of a complete replacement of one logic with another, as if different institutional domains and beliefs operate in isolation from one another. Instead, a blended logics approach to studying institutional change processes involves exploring negotiation and conflict between multiple economic, political and social actors as they interact to find new compromises and governance structures to encompass joint concerns.

As applied to the study of security and business, I suggest that one effect of a transnational terrorist event is that the security logics and actors enter into a negotiation with other political and economic actors to reconsider the proper role of security in existing political and economic systems. An important point of the institutional change literature is that these types of changes are not punctuated in the sense that there is a direct correspondence between a terrorist event and security-dictated changes into existing institutional structures. Instead, a terrorist event initiates a process of change that is likely to take a long time as initial ideas cascade into concrete actions. The primary research goal of my study is to explore these processes over time to better understand the long-term effects of a major transnational terrorist event on security-related institutional changes for business.

To accomplish this goal, the terrorist event that I explore is the September 11, 2001 terrorist attack. As the 9/11 Commission Report remarks, "[t]his pattern has occurred before… The United States faces a sudden crisis and summons a tremendous exertion of national energy. Then, as that surge transforms the landscape, comes a time

for reflection and reevaluation. Some programs and even agencies are discarded; others are invented or redesigned. Private firms and engaged citizens redefine their relationships with government" (National Commission, 2004, 361). In the aftermath of 9/11, we saw massive public structural and organizational changes with the creation of the Department of Homeland Security, new agencies like the Transportation Security Administration, and experimental public private partnerships like the Area Maritime Security Councils. We also saw massive public investments in heightened airport security, particularly given that the smuggling of weapons onto planes was a direct enabler of the terrorist events. In this case, TSA nationalized the airport passenger screening process as public policy concerns initiated a direct takeover of the governance structure of airport security. We also saw other changes initiated including increasing border security as well as strong investments into hardening cockpits, air marshals, and a host of other security initiatives.

While the governance changes in airports are apparent to anyone who flies, the questions this dissertation explores are related but different: How do general concerns over the security of airports following 9/11 lead to the transfer of security logics to the related critical infrastructure of seaports? Did the types of governance changes initiated by the newly founded Department of Homeland Security transpose directly into the governance of seaports? If not, then how did the construction of new security logics on seaports following 9/11 differ and why? The juxtaposition between airports and seaports in terms of the role of security logics in institutional change represents a compelling case to gain new theoretical insights into long-term processes of institutional change across multiple settings. I explore whether a transnational terrorist event leads to security-

related institutional changes that extend beyond the direct target of any particular attack. In this case, the issue relates to whether the broad concern over security translates in the same way to the critical infrastructure of seaports as it did to growing security controls over airports.

To address these questions, I developed a grounded research methodology (Glaser & Strauss, 1967; Strauss & Corbin, 1990; Kenny & Fourie, 2014). I first engaged in a process of data gathering in which I both found primary and secondary sources about the transformation of security protocols and initiatives in seaports in the decade following 9/11. I also engaged in primary interviews of individuals directly related to these processes. I conducted 45 recorded interviews and many others where the subject matter expert requested no recording for security purposes. Most interviewees requested anonymity so wherever possible I cite the interviewee's name but in some cases they are identified by number only. In several instances, the use of personal pronouns is modified to obscure the identity of the speaker.

Through my research and interviews, I identified two major institutional experiments in seaport security that further focused my research design: (1) Transportation Worker Identity Credential and (2) Area Maritime Security Plans.

The Transportation Worker Identify Credential (TWIC) was an initiative to strengthen security protocols over what type of employees were able to enter all transportation hubs (*e.g.,* seaports, airports, rail, etc.), but the introduction of these credentials were first (and to this day, primarily) introduced to increase security protocols at seaports. A particular feature of the TWIC initiative is that it was introduced and

controlled by the Department of Homeland Security. In the same way that the federal government took over the security of who was allowed to enter airports, it also introduced a massive effort to at least control who was granted identify cards to enter the secure area of seaports. However, the governance structure was limited and the private sector retained portions of access control oftentimes as an unfunded mandate.

The second initiative related to the development of Area Maritime Security Plans (AMSPs) and Facility Security Plans (FSP) that defined the exact boundaries of what parts of the seaport were considered to be security critical, how these areas were identified and marked, and who was to monitor and enforce these security boundaries. The TWIC and AMSP/FSPs were strongly interconnected: the TWIC represented an effort to identify who should be able to enter secure areas of the ports, while the AMSP/FSPs represented the effort to define which parts of the port should be accessible only by those who hold TWICs and who should be responsible for monitoring those borders.

An interesting outcome of comparing the long-term implementation of both the TWIC and the AMSP/FSPs rests in the different strategies of security-related institutional based changes pursued by the various actors. The TWIC represented a case where the strategic intent represented what the academic literature defines as a process of "replacement" of institutional structures (Purdy & Gray, 2009). From this perspective, institutional change is viewed as rapid and wholesale: an old institutional structure governed by existing players is simply replaced by a new structure governed with new actors. As applied to this case, this nationalization strategy applies to the intended goals of the Department of Homeland Security to directly control and centralize the process of

security identification of seaports. In the same way that the Department of Homeland Security came to take over the security of entrance into airports, so did it claim control over the control of TWIC at seaports. The security over the identification cards was perceived as a public good that was best directly controlled by federal security actors.

In contrast, the implementation of the AMSPs represented a completely different approach to the introduction of security-related governance changes within seaports. Central to the implementation of this security initiative were public-private partnership organizations called Area Maritime Security Committees (AMSCs). In this case, security actors did not take over the introduction of a new function, but instead acted to guide private actors within the maritime industry to develop their own security plans to assess various potential threats and separate those maritime activities most prone to terrorist attacks from other less sensitive areas. This approach reflects what the literature calls a "blended" or "hybrid" approach to institutional-based change (Skelcher & Smith, 2015; York, Hargrave & Pacheco, 2016). The strategic intent was not to replace existing governance structures with a new security logic, but instead to have private and public actors work in tandem to develop new plans that provided new boundaries between the public good, in this case represented by collective concerns over security, and the private good, in this case represented by the concerns of the private terminal owners to run their operations with as few energies and costs dedicated to the protection of security as possible.

Based on a long-term analysis of the eventual implementation of these two programs over the first 10+ years following September 11th, the concluding chapter offers a number of propositions about the effects of a transnational terrorism event on

institutional change in the private critical infrastructure section. First, I propose that viewing the emergence of a new security logic in business as solely the responsibility of public actors misses the immense challenge of grafting new security logics into existing economic systems. A public sector replacement strategy, such as the example of the TWIC examined here, required more resources and investments than original policy designers were willing to make, and even then, involved a careful balancing of security and economic logics in its implementation that, to this day, has never been fully addressed.

In contrast, I propose viewing security-related institutional change not as the replacement of one type of logic with another – a full scale replacement of an economic logic with a security one, for instance – but instead as a blending activity of negotiation and change that takes place at the boundaries of business and security. The case of the emergence of the security plans that came out of the direct negotiations in the AMSCs illustrates the benefits of cross-sectoral collaboration in the implementation of new security objectives. These committees did not aim to replace one logic with another, but instead to develop and deploy new responsibilities given the collective threat and cost to all actors of a possible terrorist attack. Similarly, I propose that exploring the effects of terrorism on business requires a similar focus on the intersection of multiple logics that lead to significant institutional changes following a major terrorist event. Long-term, sustainable security-related change lies at the intersection of political, economic and security logics as institutional responsibilities are debated and redrawn in the face of an increasingly risky global business environment.

CHAPTER 1: TERRORISM, SECURITY AND THE CONSEQUENCES FOR BUSINESS: SIGNIFICANCE AND RESEARCH QUESTIONS

1.1 INTRODUCTION

The blue skies of September 2001 were marred by the smoke and flames of multiple terrorist incidents perpetrated against both the public and private sector. The busy streets of Mumbai were filled with carnage in and around the Taj Mahal Palace Hotel after an attack by Pakistani terrorists in 2008. The normally lively streets of Paris at dinnertime were shattered by the chatter of automatic weapons fire in November 2015. Countless other terror-related incidents have taken place throughout the world, increasingly targeting private-sector interests. These large-scale, punctuated terror events tend to galvanize public opinion both domestically and abroad as we see social media light up with photo montages of contemplative vigils for the victims. However, the series of security-related responses oftentimes put into motion by these punctuated events have ramifications for years to come - long after the last piece of broken glass has been swept away. Policies intended to address the threat are confronted with the reality of implementation as the sudden shock of sentimentality erodes with the passage of time.

While we know that security is likely to matter more in the immediate aftermath of a terror attack, less research has been done that maintains a lens on the outcomes of these events over a long period of time. There might be congressional hearings,

presidential statements and even new laws and measures introduced and/or implemented. However, the true costs of these reactions remain elusive. The question of the manner with which security concerns (following punctuated transnational security events) eventually shape economic activity remains *under-researched*. Particularly important is the manner with which propitious security programs become sustainable. Public sector institutions propose, promulgate and even regulate security programs but when the burden falls on the private sector, public sector security logics may conflict with private sector market logics. How are these institutional boundaries determined and under what conditions do the logics interact with each other?

In this chapter, I first explore the political and economic significance of terrorism as a critical issue in the study of the interrelationship between business and society. I then turn to a review of the existing literature of terrorism and business in the management literature, but also identify the lack of focus on terrorism as an event that initiates long-term institutional change as a primary gap in the extant literature.

I then review research into the role of institutional logics in society to fill this gap of security-related research in the business literature. From this perspective, I view security as an ideal type institutional logic that exists as a primary force in the structuring of the state and the economy; striving for security defines the mission of major institutional pillars in our society, particularly by military and security-related officers and organizations that receive significant investment and support. However, the study of security is not isolated to specialized military agents or law enforcement organizations. Terrorism raises the salience of the security logics across multiple societal domains, including the economic, thus contributing to a process of institutional debate and change

that extends beyond any of the direct consequences of the costs of any single terrorist event. In my review of the literature that reviews the interaction of multiple logics in action as a source of institutional change, I propose that the study of terroristic attack consequences therefore requires looking at the manner with which concerns for security spill over to debates over the proper boundaries between public and private actors which includes the participation of political, security and economic actors.

1.2 Terrorism and Business

Terrorism is one of multiple types of threats that arise from a general concern for the overall security of a firm.[1] For definitional purposes, security threats are those forces (man-made or natural) that can damage or destroy firm assets including physical, cyber, intellectual, and human resources. Natural threats include weather-related security concerns such as hurricanes, flooding and earthquakes. Man-made threats include issues of cyber security, corporate espionage and sabotage, unauthorized use of intellectual disturbances, civil and military conflict, and terrorism.

Terrorism, one of many types of security threats facing firms, is designed to sow fear and cause damage amongst the public-at-large. More specifically, terrorism is the use of violence, usually to achieve social or political goals, with the following frequently conjoined characteristics: (1) violence is designed to create terror, fear, or panic in a population; (2) the use of violence is usually random or arbitrary; and (3) non-combatants or "innocents" are often the target (Morris & Frey, 1991).

[1] See Appendix A for an extended review of threats facing firms.

Terrorism lurks specifically at a critical point of intersection in the study of business and society because this type of warfare, coupled with the rise of non-state actors, has increasingly pronounced the private sector as legitimate targets by those wishing to harm a society's institutions. All of the firms' assets are potential targets with respect to terrorism. People, customers, financial stability, physical assets and even stock prices can be deliberately targeted. As discussed in more depth in subsequent sections, critical infrastructure organizations, such as privately-owned energy utilities or transportation hubs (airports, railroads, seaports, etc.) represent particularly rich targets for terrorism because of the ripple effects of the economic consequences of a lack of public confidence in their secure operations and/or the very real damage that occur to both society and the economy should these system of systems fail.

For instance, consider the cascading economic costs of the September 11 terrorist attacks versus simply the physical damage caused that day. The operation cost Al Qaeda approximately $500,000 by most estimates. If one were to include the total capital loss of related stock market volatility, the true long term effect of this punctuated transnational terror attack is likely more than $2 trillion (Institute, n.d.). According to the Institute for the Analysis of Global Security, estimates for 9/11 expenditures for the United States alone, not considering market losses, total approximately $240 billion. These figures include costs such as the loss of aircraft, replacement cost of the World Trade Center buildings, cleanup costs, lost wages of workers directly affected, and others as detailed in Table 1.1, provided at the end of this chapter.

These types of economic externalities of transnational terrorism are often one of the direct reasons why enemies of a particular country engage in terrorist strikes. For

instance, in the days leading up to the 2004 Presidential election, Osama bin Laden (then leader of Al Qaeda) released a telling statement that explained his justification and desire to continue his policy of bleeding America to the point of bankruptcy. Bin Laden explained,

> as we [Al Qaeda], alongside the mujahidin, bled Russia for 10 years, until it went bankrupt and was forced to withdraw in defeat….So we are continuing this policy in bleeding America to the point of bankruptcy… for example, al-Qaida spent $500,000 on the event [9/11], while America, in the incident and its aftermath, lost - according to the lowest estimate - more than $500 billion (bin Laden, 2004).

From his perspective of causing maximum pain to his enemies, Osama Bin Laden's estimate that a $500,000 investment can cause losses of over $500 billion would have to be considered a sound, financial investment from a terrorist's point of view. Unfortunately, Bin Laden was not alone in making this estimation.

For the purpose of this dissertation, I further distinguish between transnational terrorism and domestic terrorism. According to a 2010 working paper on domestic versus transnational terrorism, the long-term study of the "impact of terrorism on economic growth necessitates a distinction between domestic and transnational terrorist events, because the latter can have a larger influence by scaring away growth-promoting foreign direct investment and requiring expensive border defenses" (Enders, Sandler, & Gaibulloev, 2010).

Thus, the potential consequence of transnational terrorism extends beyond losses in any one country but also to all the potential international trade that is potentially lost when national borders become more strongly protected - not to mention uncertainty in the financial markets. The effects of transnational terrorism, therefore, influence debates on

the participation of foreigners in domestic economic markets since many believe that foreign actors and owners represent a stronger security risk than domestic ones. For instance, the domestic debate over whether Dubai Ports World (DPW), a foreign-owned terminal management company, should be allowed to assume management of certain port operations was closely tied to the broader discussion of foreign ownership and security in the U.S. economy. This will be discussed in detail in subsequent chapters of this dissertation. A monetary estimate of the cumulative losses of lack of foreign investment, or withdrawal of foreign investment, due to reactionary protectionist policies is difficult to directly calculate.

1.3 Critical Infrastructure: In the Crosshairs of Terrorism and Business

Considering the growing threats and costs of transnational terrorism, it is evident that the public and private sectors, as well as society at large, share concerns regarding security. However, the issues that define the tight connections between business and security are particularly salient for the owners, operators and guardians of what is often defined as "critical infrastructure." An evaluation of past transnational terrorism incidents and experiences around the world, coupled with intelligence gathered from potential terrorist organizations, demonstrates that critical infrastructure is considered to be both valuable (in the sense of high visibility and maximum economic damage) and a vulnerable soft target[2].

[2] Soft targets refer to undefended targets that present little or no resistance to would-be aggressors.

Given these security considerations, and the systemic economic consequences of any imposed damage, the United States' security apparatus specifically targets the protection of these types of infrastructural organizations as part of their homeland security planning. The U.S. Department of Homeland Security (DHS) defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (White House, Office of Homeland Security, 2007). Likewise, as early as 2005, the Homeland Security Advisory Council (HSAC) concluded that the "[c]reation of more resilient critical infrastructures will require unprecedented collaboration and cooperation between disparate stakeholder communities" (U.S. Dept of Homeland Security, 2006, 11). The policies and national strategies for homeland security are presented in Appendix A. Appendix A illustrates the significant energies that public policy officials and security professionals have spent on the issue of securing critical infrastructure from terrorist attacks.

Thus, critical infrastructure, spanning entire countries with multiple points of failure and cascading effects when struck, are highly desirable targets for terrorists. We have seen this play out multiple times in recent years specifically against electrical grids and oil pipelines on the Arabian Peninsula. In 2013, the Yemeni power grid was attacked (similar to previous attacks by Al Qaeda), resulting in most of the country experiencing a prolonged total blackout (*see e.g.,* Ghobari & Sleiman, 2013). Subsequent attacks have left Yemen in a total blackout causing much disruption and economic damage. Attacks like this are a threat to the United States, as well. Also in 2013, perpetrator(s) severed

power lines and destroyed key pieces of equipment at the Pacific Gas & Electric (PG&E) Metcalf substation in California, demonstrating the vulnerability of the U.S. electrical grid. Some speculate that a complete destruction of this substation could have thrown San Francisco and Silicon Valley into total darkness for months. For security reasons, the full extent of potential damage to the grid will never be made public but PG&E announced thereafter that it was investing $100 million into hardening its facilities (Baker, 2014).

The U.S. Customs and Border Patrol (CBP) used the graphic represented in Figure 1.1 to illustrate the many vulnerable points and weak links that transportation infrastructure creates in the global supply chain. One begins to see the complexity of the various components and the challenge to security that these components represent.

Critical transportation infrastructure has the potential to impact global supply chains that operate across the world. One need only imagine the cascading effect of a scenario in which a large ship were deliberately sunk blocking channel traffic into and out of one of our nations' largest seaports. As a conduit for international movement of goods and people, seaports by necessity operate at the intersection of global trade. The cascading effect of a terrorist incident would have profound impact on myriad aspects of life as we know it today. With fuel, food and medical supplies available to the public measured in days rather than months, the effects of a pro-longed seaport shut-down due to an incident at a major seaport would have immediate consequences for the integration of supply chains around the world.

One of the largest challenges facing U.S. public sector national security strategists is that of protecting these types of critical infrastructure organizations in the United States. The reason is that 85% of the critical infrastructure[3] is owned and/or operated by the private sector, not the public sector (National Commission, 2004). The issue is not just of state-led security actors dictating public policies to organizations run and owned by private sector actors, but also relate to the challenge of managing the boundaries of the mix of public and private goods and incentives found in the management of privately-owned critical infrastructure.

To comprehend the ubiquitous interconnection of public and private actors in the protection of critical infrastructure, the Transportation Research Board of the National Academies produced a report following 9/11 outlining some of the key challenges associated with transportation infrastructure. That report warned:

> The U.S. highway system consists of 4 million interconnected miles of paved roadway, including more than 45,000 miles of Interstate freeway and 600,000 bridges. Freight rail networks extend for more than 300,000 miles, and commuter and urban rail systems cover some 10,000 miles. Even the more contained civil aviation system has around 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks also contain many other fixed facilities, such as terminals, navigation aids, switchyards, locks, maintenance bases, and operation control centers. Most of this infrastructure is unguarded and sometimes unattended. Distributed over the networks are millions of vehicles and containers. These vehicles and containers are repeatedly moved from one location to another,

[3]Throughout this study I refer to the statistic that 85% of the critical infrastructure in the United States is owned or operated by the private sector. This statistic can be found in dozens and possibly hundreds of texts, reports, speeches, and a host of other sources. After thorough investigation during this research, I have determined that this number is likely inaccurate despite its continued overuse in most public sector publications. Additional study to determine the true nature of private versus public sector ownership/governance of critical infrastructure is sorely needed but will remain outside the scope of this dissertation. I was told that several years ago, a Ph.D. student was researching this statistic but I have been unable to locate her findings to date. Nevertheless, as this statistic is in perpetual use by the government, I will employ it here as well.

> complicating the task of monitoring, safeguarding, and controlling them (Transportation Research Board, 2002).

This does not even take into consideration the entire transportation system. When one considers the scope and size of the nation's critical infrastructure, there can be little wonder why the government sector relies so heavily on the private sector for ensuring some modicum of security over this system of systems. The diversity of actors, fields, industries, firms, governments, special interest groups, stakeholders, shareholders and myriad other interested parties ensure a range of ideas and proposals in terms of security.

Given these complexities, the governance of any individual critical infrastructure organization – *e.g.*, a single port, airline or railroad – is best perceived as sitting at the intersection of public and private goals and incentives. As the primary role of government is to provide security, it is hindered by limited cognitive ability, limited resources, and limited information. All of the aforementioned contribute to critical infrastructure protection being a seemingly impossible task. Likewise, since so much of the infrastructure is owned by the private sector, the government must rely on the private sector to either share its vulnerabilities and/or to share in allocating the necessary resources to ensure resiliency of the infrastructure. Both are fraught with innumerable pitfalls. How would the government keep the vulnerability information safe? How does the public sector incentivize the private sector to allocate its own resources to critical infrastructure protection? Which definition of security do the various stakeholders use? What is a priority national security asset for the federal government, for example, which also may rank low when one considers the same asset from an economic perspective at the state government level?

At the same time, firms must deal with political risk associated with critical infrastructure both in their home country and in their respective host countries. Expenditures for security may make a firm less competitive if its competitors are investing using market logics rather than security logics. If security were left to the private sector alone, no single company could amass the same security force and matériel as does the government. Likewise, the public at large would likely not welcome large security forces visible throughout their daily lives.

From a national economic perspective, not only is ensuring sustainable competitiveness an important distinction for both the public and private sectors, so also is business continuity. The resilience of both the public and private sectors to return to operations following an incident is paramount to long-term survivability. Business continuity is defined as the "capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident" (ISO, 2012). Between 2004 and 2006, the HSAC tackled many of these issues and produced several noteworthy reports in the years following 9/11. For example, information sharing between the public and private sectors seems relatively straight-forward at face value. The government is interested in the private sector's critical infrastructure vulnerabilities, weak links in supply chains, net effect of cascading failures as one infrastructure oftentimes relies on others, and a host of other similar issues; however, the private sector is concerned that the same information could be used by competitors as a competitive advantage or picked up by the wrong hands and used against the company itself.

As such, the role of the private sector in protecting and ensuring security remains an important component in the research involving the long term effects of transnational

terrorism, particularly critical infrastructure organizations. To address these issues, I first review the existing literature on terrorism in the business literature. I then look into the research gaps with a focus on the public-private interface that shapes the scale and complexity of the effects of transnational terrorism on patterns of institutional change for business over time, particularly as related to the management and governance of critical infrastructure organizations.

1.4 Literature Review

In a 2004 edited anthology entitled *Terrorism and the International Business Environment*, Michael Czinkota, Gary Knight and Peter Liesch wrote a chapter providing early conceptual foundations for terrorism-related research. Writing about the challenge of terrorism-related research from an international business perspective, they wrote that "terrorism is a relatively nebulous or imprecise construct, whose nature, antecedents and consequences may be difficult to conceptualize or distinguish from other events that occur in the macro environment of business" (Czinkota, Knight & Liesch, 2004, 48). They proceeded to outline three levels of research: (1) primary, or research on the level of the individual firm; (2) macro, or research on the level of the global environment; and (3) micro, or research on specific regions, industries or levels in international value chains (Czinkota, Knight, & Liesch, 2004).

1.4.1 Terrorism in the Business Literature

While identifying the possibility of an extended research topic, most existing research in the business literature falls under category of what Czinkota, *et al.* define as "primary" research at the level of a firm. A variety of other papers have considered

various aspects of terrorism and business from this perspective, including businesses responses to terrorism (Frey, 2009); effects of international diversification on the consequences of terrorism for individual multinational firms (Li *et al.*, 2008); cost of terrorism insurance (Kunreuther, 2002); consequence of terrorism on supply chain management (Sheffi, 2002); effects on Italian employment (Greenbaum, Dugan & LaFree, 2007); price of real estate in central business districts (Abadie & Dermisi, 2008); and impact of cross-national variation in terrorist events on foreign direct investment (FDI) (Powers & Choi, 2012).

Czinkota, Knight, Liesch & Steen (2010) further propose that a research agenda on business and terrorism can be furthered "by developing integrated risk management models that account for terrorism risk within corporate strategy" (p. 838). They suggest viewing terrorism security at the level of an individual firm as a form of political risk that companies wish to actively manage, especially those companies that operate in industries particularly at risk of attack given their potential externalities as terroristic targets. Czinkota, *et al.* (2010) also suggest that viewing security as a form of managing legitimacy provides an alternative lens by which to further extend firm-level studies into this topic. Firm incentives to manage terrorist events include the activity of managing and sustaining its efforts to establish its legitimacy among relevant constituents or else face potential new costs to government oversight stemming from new the introduction of new security-related improvements. For instance, these authors state that security improvements "especially in the infrastructure of international transportation, logistics, communication and information technology", combined with "new measures such as

the… Maritime Transportation Security Act… have imposed tens of billions of dollars in compliance and other costs on private sector firms" (Czinkota, *et al.*, 2010, 831).

1.4.2 Institutional Change as a Research Gap

Overall, existing research in the field of business primarily takes a firm-level view on managing relatively well-known security concerns focusing on issues such as political risk and legitimacy at the level of a single firm. These insights provide important contributions into why corporations should care about the direct effects of terrorism on their individual firms. However, the existing theoretical frameworks have a strong gap that misses at least one important consequence of transnational terrorist effects on business outcomes: the potential effects of terrorism on changing the underlying rules of the game in both domestic and international business. The impact of terrorism on business is not borne solely by those companies that are attacked but also by firms across multiple markets and industries that are likely to face the repercussions and spillovers of political and social responses to increasing security concerns.

Consider the 2015-16 terror attacks across Europe. In their aftermath, European governments struggled to balance the needs of the mobile labor force with the free flow of potential terrorists. Thus, transnational terrorism had a profound impact on global labor mobility as politicians across many European countries justified closing borders in light of security concerns, despite long-held agreements signed under the Schengen Agreement to retain open labor mobility throughout the European Union. In this case, the institutional rules that defined the Schengen Area traditionally have drawn concern and are now questioned for their viability via security.

Similarly, in the aftermath of the September 11 attacks in the United States, we have seen the U.S. Transportation Security Administration (TSA) nationalize the entire security function at airports to avoid a prolonged economic catastrophe of passengers refusing to reboard aircraft (effectively a combination border closure/internal movement stop). Effectively, nationalization of the airport security function demonstrates the coalescence of multiple logics manifested in federal security workers replacing private contractors at security. The nationalization of airport security was wholesale and includes the replacement of private contractors with federally funded and supervised security officers. This change is not only in the rules of airport security, such as what can be brought onto a plane, but also in the agents and processes designed to successfully implement those policies.

Given the wide-reaching and long-term effects that transnational terrorism may bring to the institutional environment, the business and firm-level models that look at costs, risks and legitimacy of individual firms do not provide a sufficiently wide lens to grasp the complexities of the full range of large-scale consequences of terrorist events on business activities. To fill that gap, I explore in the next chapter the concept of institutional logics as an alternative theoretical framework to explore the complex relationship between business and society.

1.4.3 An Institutional Logics Perspective: The Ideal type Security Logic

To apply an institutional perspective on the study of terrorism and business, I first build on the research in the institutional logics literature. Institutional logics are defined as sets of material practices and symbolic constructions which constitute societies'

organizing principles (Friedland & Alford, 1991; Thornton & Ocasio, 2008; Thornton, Ocasio & Lounsboury, 2012). While this literature has defined six ideal logics (family, religion, state, market, profession, and corporation), one contribution of my research is to introduce a seventh ideal type security logic. Friedland and Alford (1991) wrote of six central institutions that shape individual interests and organizational preferences. They viewed institutions as both "supra-organizational patterns of activity through which humans conduct their material life in time and space, and symbolic systems through which they categorize that activity and infuse it with meaning" (Friedland & Alford, 1991).

Thornton, *et al.* (2012) then applied these six central institutions as the foundation for their institutional logics ideal types. However, a gap in their mapping of institutional domains is that they do not include an explicit analysis of security concerns and personnel as an independent logic. They propose that the ideal type classification of institutional domains can more fully serve as "theoretical model[s] for how the boundaries of the institutional orders are systematically defined and identified" (Thornton, *et al.*, 2012, 53). Further, ideal types are

> not a description of an organizational field, research context, or level of analysis. They are an abstract model used to gauge the relative distance of the observations from the pure form to the ideal type. In theory this distance can be used to predict some outcome variable, though we are in need of methods development research on how to quantify the distance. An ideal type is not a hypothesis, but it offers guidance in the construction of hypotheses. An ideal type is not an average type nor does "ideal" imply approval (Thornton, *et al.*, 2012, 53).

I suggest security does not rest comfortably embedded within pre-existing ideal types. In the existing framework, the state is tied to the redistribution in the economy rather than its control of the monopoly over force. Nor is the control of a military to protect the public good of the security of its borders and people, or as law enforcement for preservation of society at the sub-national level, fully discussed in the existing state logics that focus on the redistributory role of the state in society. In contrast, more than simply redistribution, the act of defending society itself is the driving concept of security for which the state exists at its most fundamental level.

As A.H. Maslow (1943) described, security is as fundamental to the continued existence of the society and/or the firm as it is to the human condition. Whereas Maslow warns,

> again, as in the hungry man, we find that the dominating goal [of safety] is a strong determinant not only of his current world-outlook and philosophy but also of his philosophy of the future. Practically everything looks less important than safety, (even sometimes the physiological needs which being satisfied, are now underestimated). A man, in this state, if it is extreme enough and chronic enough, may be characterized as living almost for safety alone (Maslow, 1943).

Clearly, both society and firms must maintain a sense of security if simply for the preservation of self and various mechanisms (*e.g.,* critical infrastructure) required to ensure their very existence. The underlying need for security as an ideal type within the broader spectrum of institutional logics becomes evident in that the ideal types "convey what is essential about a phenomenon" and can "accommodate integration of theory at multiple levels of analysis," thereby increasing generalizability and accuracy (Thornton, *et al.*, 2012). Further, the addition of security as an ideal type enables the researcher to

better form a theoretical model for "how the boundaries of the institutional orders are systematically defined and identified" (Thornton, *et al.*, 2012).

Therefore, to accomplish my research goal of directly studying processes of security-related institutional change, I propose that a "security" logic be added as an "ideal type" into the existing categorization of domains presently discussed in the institutional logics literature. Similar to Friedland and Alford (1991), I view security as that same "supra-organizational pattern of activity" through which we can better understand the actions, motivations and interrelationships of society and firms. My intent is to explore the salience of a separate security logic as a means to understanding the ways that transnational terrorist events can initiate a process of institutional change where the particular concern of these issues become salient in public discourse and policy.

As illustrated in Table 1.2, I therefore propose expanding the six ideal types to include a seventh: security. According to Thornton, *et al.* (2012), the y-axis is composed of "building blocks specify[ing] the organizing principles that shape individual and organizational preferences and interests and the repertoire of behaviors by which interests and preferences are attained within the sphere of influence of a specific order" (Thornton, *et al.*, 2012). Thus, not only are we setting the conditions to better study security, but also unbundling the concept of security as an abstract construct to include those ideals, agencies and actors specifically designed to defend it in a modern economy.

1.4.4 Logic Hybridization as a Process of Institutional Change: Implications for Security

The emerging research field of blended and hybrid logics offers new insights into the processes and outcomes of security-based institutional change that other research

streams cannot convey. Unlike other research streams about institutional change where social movements (McAdam, 1982), institutional entrepreneurship (Garud, Jain & Kuwaraswarmy, 2002) or collective action models (Hargrave & Van de Ven, 2006), for example, do not adequately provide insight into security-based change, institutional logics provide a more robust theoretical framework by which to explore the role of security logics in shaping institutional outcomes of terrorist events. This research stream includes works on institutional logics and institutional change in organizations (Thornton, Jones & Kury, 2005); conflicting logics and multilevel dynamics (Purdy & Gray, 2009); field level institutional change (Thornton, Ocasio & Lounsbury, 2012); logics hybridity (Skelcher & Smith, 2015); and most recently, logic hybridization and integration of previously incompatible logics (York, Hargrave and Pacheco, 2016). This research relaxes an assumption found in many earlier firm-level studies of logics that the boundaries between different institutional domains are themselves fixed or static over time. In contrast, these authors explore the intersection of alternative logics as a force of long-term institutional change. Institutions change as alternative logics, and the societal actors assigned to protect them, come together to create practices that reflect a compromise or blending of existing logics that pushes joint strategies and outcomes in new directions. Thus, in contrast to studies that delve into *ideal types* in isolation from other institutional logics, these researchers look at logics in action as a force of change rather than only stability.

From this perspective, the issue in understanding change process is not simply to identify why some members of society might call for a new type of institutional change, such as strengthening the rules that protect the security of critical infrastructure

organizations, but also identify the ways that prescriptive calls for new directions interact with existing institutional logics and structures in shaping realized outcomes. For instance, Purdy and Gray (2009), in their study of state differences in the structure of dispute resolution offices across the United States, reference Holm's (1995) basic insight that "[n]ew institutions are not created from scratch but are built upon older institutions and must replace or push back preexisting institutional forms" (Holm, 1995). According to Purdy and Gray (2009), ideal type institutional logics are not deployed fully formed but become part of the toolkit of actions as various individuals mobilize to try to enact change within preexisting networks of interests, actors and beliefs.

To advance research into examining institutional hybridity, Purdy and Gray (2009) propose an initial typology to categorize the way in which a new logic may come to influence an existing institutional field: transformation, grafting, bridging and exit. *Transformation* refers to situations in which a desired new institutional logic came to replace existing practices; others call this a "replacement" outcome, as one institutional logic is simply replaced by another (Thornton, Lounsboury & Ocasio, 2012). Purdy and Gray (2009) identify another outcome of conflicting institutional logics as *grafting*. Rather than replacing existing practices, the new logic comes to be placed at the periphery of existing dominant logics. The new logic does not transform the core of the existing system but instead becomes incorporated within existing logics without changing core beliefs or practices. The idea of "symbolic" implementation illustrate what Purdy and Gray (2009) describe as grafting in which new ideas are ceremoniously accepted for external legitimacy but do not penetrate into the substantive activity of the existing institutional structures. A third type of institutional hybridity is referred to as *bridging*,

which represents an attempt to find a compromise between new and old institutional structure such that the compromised outcomes requires deviations from ideal type institutional concerns. In this case, the implementation of new logics relates to substantive changes in actual activities over time rather than solely ceremonial adoption. Finally, the fourth strategy is *exit*. In some cases, the transposition of a new logic onto existing structures simply fails to be implemented over time, no matter the intent or motivation of those that called for such changes.

Thornton, Ocasio and Lounsbury (2012, 164) further elaborate on these different categories of institutional hybridity. As seen in Table 1.3, these authors build on Purdy and Gray's work to first distinguish between cases of *transformational* and *developmental* cases of change. Under the category of *transformational* change, they include the cases of replacement and blending but also introduce the concept of a segregated case of institutional hybridity, where both logics exist but remain fully separated from each other in their implementation. Under the case of *developmental* change of institutional dynamics, they define more incremental than more transformative changes. Included in this are processes of assimilation, elaboration and expansion/contraction that "maintain the majority of prevailing practices and symbolic representations" (Thornton, *et al*., 2012).

Most recently, building on these concepts in a further elaboration of the role of logics in shaping both the processes and outcomes of institutional change, we find hybridity emerging within the field (Skelcher and Smith (2015); York, Hargrave and Pacheco (2016)). These authors differentiate between *hybridization* and *blending* as ways in which distinct logics co-inhabit a similar institutional field. They propose that

logic hybridization "differs from blending [in the Thornton, *et al.*, 2012 usage] in that the goals of incompatible logics are integrated as complementary; they do not merely coexist. … [Instead], hybridization processes change the relationship between incompatible logics, eventually leading to a new hybridized logic that integrates the incompatible logics" (York, *et al.*, 2016, 583). That is, hybridization reflects an outcome in which new logics can emerge that encompass elements of both new and existing beliefs and practices (York, *et al.*, 2016, 583).

1.4.5 Research Questions: Security Logics in Practice

The existing research into institutional blending and hybridization raises important questions for the study of security logics in practice. In contrast to studies that delve into *ideal types* in isolation from other institutional logics, my research design considers the effects of security logics in tension with alternative forces and perspectives. For instance, the public sector is likely to view security in terms of their primary logics of ensuring stability, saving lives and securing votes, whereas the private sector sees security in terms of profitability, costs and risks. In contrast, an institutional hybridization perspective is likely to look at the ways, if any, these different definitions and meanings given to security come to interact over time to lead to actual substantive changes in the institutional environment of business. On one hand, calls for new types of security-led institutional change may simply become forgotten over time as the public's interest turns to new issues and topics, leading to the type of outcomes identified as "exit" (Purdy & Gray) or "blocked" (Skelcher & Smith, 2015) in the institutional hybridity literature. On the other hand, the calls for increased security that inevitably follow large,

transnational terrorist events may initiate substantive changes to the institutional environment for business that range from the transformational to the incremental.

A strong motivation of the dissertation is to advance our understanding of logic hybridization as a process of security-based institutional change. As a beginning working hypothesis, I propose that a transnational terrorist event on a private-sector target is likely to lead to the increasing salience of security as a growing concern for both public and private actors. The question I wish to explore is how the increasing salience of the security logics interacts with existing institutional structures and beliefs to shape substantive change over time.

In so doing, I wish to move beyond theories that look at the intersection of business and security as separated institutional domains. That is, an explanation of the effects of security on business can be fully understood solely through an analysis of the actors that inhabit non-economic institutional settings, such as those politicians and civil servants that staff the U.S. Congress or the U.S. Department of Homeland Security. Instead, I hope to include the role of economic actors in shaping "blended" or "hybrid" outcomes that sit at the intersection between security and economic logics, allowing for the possibility that outcomes may emerge that do not fully fit within in any ideal type institutional logics.

To advance these concerns, I pose the following research questions to guide my efforts in a grounded methodology to extend the literature of the role of terrorism in shaping the long-term relationship between business and security:

1. What are the long-term consequences of a punctuated transnational terrorist event on the institutional environments of business?
2. Specific to a major terror related event, how do security-based logics interact with existing political and economic institutions to produce change?
    a. What is the role of the private sector in implementing security-based institutional changes?
    b. How much do security-based institutional change strategies influence the long-term institutional environment of business?
    c. How can security-based institutional change efforts be evaluated in terms of long-term impact? What explains differences between transformational and incremental institutional change?

TABLE 1.1: COST ESTIMATE OF 9/11 AND SUBSEQUENT RELATED U.S. EXPENDITURES

$385 million	• The loss of four civilian aircraft
~$3 to 4.5 billion	• The destruction of major buildings in the World Trade Center with a replacement cost
~$1 billion	• Damage to a portion of the Pentagon
$1.3 billion	• Cleanup costs
$10 to 13 billion	• Property and infrastructure damage:
$40 billion	• Federal emergency funds (heightened airport security, sky marshals, government takeover of airport security, retrofitting aircraft with anti-terrorist devices, cost of operations in Afghanistan)
$17 billion	• Lost Wages associated with 83,000 direct job losses
$21.8 billion	• The amount of damaged or unrecoverable property
$95 billion	• Losses to the city of New York (lost jobs, lost taxes, damage to infrastructure, cleaning)
$40 billion	• Losses to the insurance industry
$10 billion	• Loss of air traffic revenue
Unknown	• Fall of global markets: incalculable.
$239 to $243.5 billion (without considering market losses)	**TOTAL ESTIMATE**

Source: Institute, n.d.

TABLE 1.2: ADDITION OF 7TH IDEAL TYPE: SECURITY

Y Axis	X Axis						
Categories	**Family**	**Religion**	**State**	**Market**	**Profession**	**Corporation**	**Security**
Root Metaphor	Family as firm	Temple as bank	Redistribution mechanism	Transaction	Relational network	Hierarchy	Preservation of Society
Sources of Legitimacy	Unconditional Loyalty	Sacredness in Society	Democratic participation	Share price	Personal Expertise	Market position of firm	Ensure survival
Sources of Authority	Patriarchal domination	Priesthood charisma	Bureaucratic domination	Shareholder activism	Professional Association	Top Management	Sworn Officers
Sources of Identity	Family reputation	Association with deities	Social and economic class	Faceless	Association with quality of craft; personal reputation	Bureaucratic roles	Uniforms and symbols
Basis of Norms	Household membership	Congregational membership	Citizenship membership	Self-Interest	Associational membership	Firm employment	Unit membership
Basis of Attention	Status in household	Relation to supernatural	Status of interest group	Status in market	Status in profession	Status in hierarchy	Formal rank achieved
Basis of Strategy	Increase family honor	Increase religious symbolism of natural events	Increase community good	Increase profit	Increase personal reputation	Increase size of firm	Continuance of society
Informal Control Mechanisms	Family politics	Worship of calling	Backroom politics	Industry analysts	Celebrity Professionals	Organization Culture	Training programs
Economic System	Family capitalism	Occidental capitalism	Welfare capitalism	Market capitalism	Personal Capitalism	Managerial capitalism	Leadership capitalism

Source: This is an adaptation of the original table of ideal types by Thornton, Ocasio and Lounsbury, 2012.

TABLE 1.3: TYPOLOGY OF CHANGE IN FIELD-LEVEL INSTITUTIONAL LOGICS

	Forms of Change	Definition	Sample Study
Transformational Change	Replacement	One institutional logic replaces another	Rao, Monin, and Durand (2003)
	Blending	Combining dimensions of diverse logics	Glynn and Lounsbury (2005)
	Segregation	Separation of logics from a common origin	Purdy and Gray (2009)
Developmental Change	Assimilation	Incorporation of external dimensions	Murray (2010)
	Elaboration	Endogenous reinforcement	Shipilov, Greve, and Rowley (2010)
	Expansion Contraction	Shift from one field to another; Decrease in logic's scope	Nigam and Ocasio (2010), Reay and Hinings (2009)

Source: Thornton, Ocasio and Lounsbury, 2012

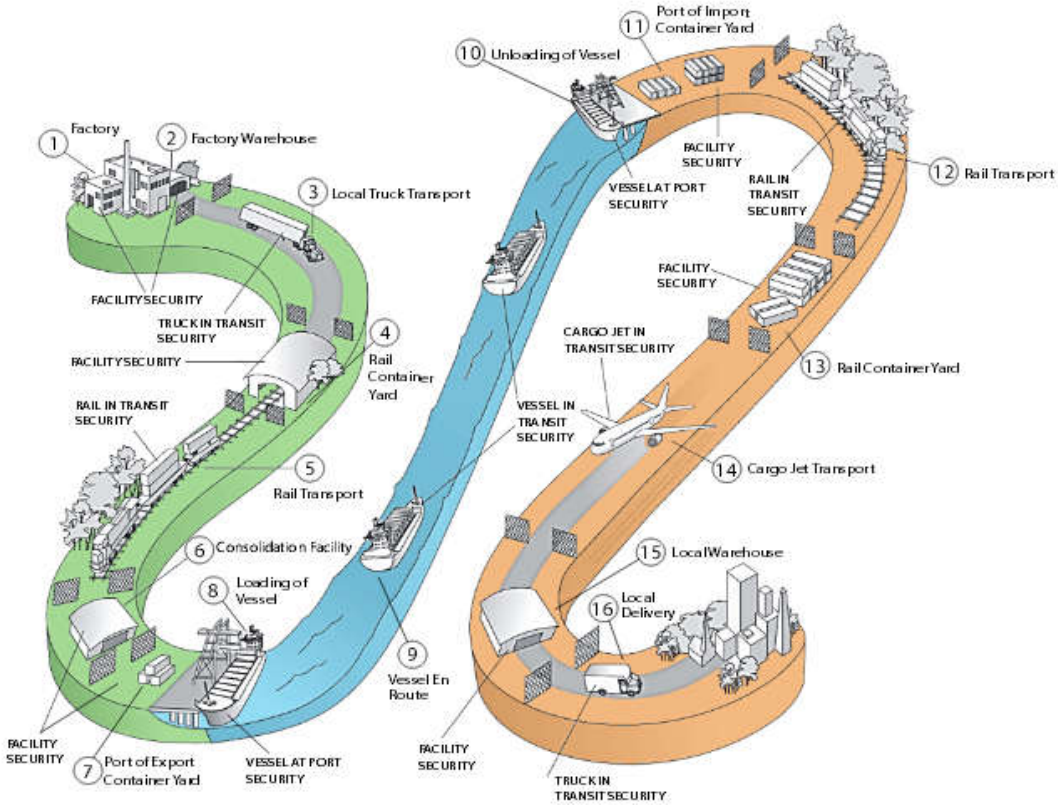


FIGURE 1.1 VULNERABILITIES IN THE GLOBAL SUPPLY CHAIN

Source: U.S. Department of Homeland Security, U.S. Customs and Border Protection, 2015

CHAPTER 2: RESEARCH CONTEXT AND METHODOLOGY

"In its Fall 2000 report, the Commission concluded that the state of security at U.S. seaports generally ranged from poor to fair, control of access to seaports or sensitive areas within seaports was often lacking, and the vulnerability of American ports to potential terrorist attacks was high" (U.S. Department of Homeland Security, Office of Inspector General, 2005).

"[T]he private sector controls 85 percent of the critical infrastructure in the nation. Indeed, unless a terrorist's target is a military or other secure government facility, the 'first' first responders will almost certainly be civilians. Homeland security and national preparedness therefore often begins with the private sector… Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. (National Commission, 2004).

2.1 INTRODUCTION

On the morning of September 11, 2001, 19 hijackers boarded four aircraft in three cities: Boston, Newark and the outskirts of Washington, D.C. (National Commission, 2004). What transpired over the next several hours had far-reaching implications – not only for the innocent victims in the air and on the ground but also for public and private sector interests around the world. All told, the total monetary cost of 9/11 has been estimated at more than $239 billion and if one takes into account the global stock market downturns resulting from the aftermath of this transnational terror incident, estimated cost increases to more than $2 trillion (Institute, n.d.). Years on from these events, we are only beginning to understand the true long-term effects on the business community and the underlying institutional logics.

To address the research questions I posed in Chapter 1, I use September 11, 2001, as the primary terrorist attack that initiated a period of internal consideration of security concerns about the security of critical infrastructure in the United States. See Appendix A for a review of the general public policy discussion on critical infrastructure that emerged during this time. In my case, I specifically focus on the effects of September 11th on activities designed to protect seaports. Thus, I deliberately wish to look beyond the direct effects of September 11th on airports (obviously the airline industry was directly involved in the attacks). Instead, I am concerned about the ways in which transnational terrorism diffuses across industry boundaries to raise broader concerns about security logics even beyond those firms and industries that were directly attacked. Seaports are hybrid organizations by their very nature. With public, private and non-profit actors involved with seaports in a variety of capacities, I believed that this type of hybrid critical infrastructure would show the long-term effects from a punctuated terror attack on various organizations and institutions within the same limited geographic area.

To fully understand logics in action and how security and economic logics collided, I chose to explore the ways that security logics became enacted in practice by multiple actors over time as the issue of security concerns intensified across critical infrastructure organizations. The political/public policy actors include members of Congress, the Presidential Administration, political staffers, state and local officials. Economic actors include the private sector, labor unions and public/private partnerships in the form of port authorities. Finally, security actors include those public sector entities whose primary function deals with security including the U.S. Coast Guard (Coast Guard), Transportation Security Administration (TSA), state and local law enforcement.

My grounded theory research methodology led me to trace the actions of these various groups in the years following 9/11 (as well as several emergent security programs in seaports) to build a better theoretical understanding of both processes and outcomes of transnational terrorist activities on the institutional rules designed to govern port security within the United States.

2.2 Background: Institutional Hybridity and Seaport Governance

Unlike many countries that have a national seaport authority that owns, overseas and manages all aspects of seaport operations, the United States has a mix of public, public-private and private seaports. With no national port authority, authority over seaports in the United States are diffused through a complex interaction between public, private and security actors. This patchwork of institutional logics and actors, therefore, represents an ideal location to study the interaction of security, political and economic logics and actors in action as they respond to a punctuated international terror event. Prior to September 11, 2001, seaports already represented a hybrid system of institutional governance. This preexisting condition opens a window through which to observe the effects of potentially growing concerns over the security institutional logics following a major act of transnational terrorism on the broader governance of the seaport as a whole. This section of the dissertation provides background information on the institutional hybridity of seaport governance before the events of September 11, 2001, to provide a baseline to follow subsequent changes in seaport governance. As depicted in Figure 2.1, there are multiple actors that constitute a seaport as a whole.

Further, Figure 2.1 identifies a complex interaction between multiple stakeholders. The "port authority" is given the task of supervising the economic tasks of coordinating the activities of multiple terminals. Port authorities may actually own all or some of the terminals, but terminals may also be owned by private actors. For instance, at a *landlord port*, the port authority builds the wharves, which it then rents or leases to a terminal operator (usually a stevedoring company). The private operator then invests in cargo-handling equipment (forklifts, cranes, etc.), hires longshore laborers to operate such lift machinery and negotiates contracts with ocean carriers (steamship services) to handle the unloading and loading of ship cargoes. See Figure 2.2 for a depiction of the landlord port arrangement.

At an *operational port* like Charleston, South Carolina, the port authority builds the wharves, owns the cranes and cargo-handling equipment and hires the labor to move cargo in the sheds and yards. A stevedore hires longshore labor to lift cargo between the ship and the dock, where the port's laborers pick it up and bring it to the storage site.

However, as Figure 2.2 illustrates, while the public management of the port as an economic entity is assigned to a Port Authority, the Coast Guard provides federal oversight of port wide safety and security. Regulations give Captains of the Port (COTP) extraordinary authorities over vessels, facilities, cargo operations, and the people that work on vessels and the waterfront. Originally created by Congress during World War I as a response to major security concerns over German saboteurs (read: foreign terrorists), the COTP role evolved throughout the 20th century to be the primary security agent in charge of seaport governance (Tucci, n.d.).

From an international trade perspective, seaport governance is also a bit arcane to the casual observer with seemingly overlapping spheres of public responsibility. Legal precedent and tradition combined to interpret and evolve the Commerce Clause of the U.S. Constitution into the basis for federal government exclusive jurisdiction and responsibility over navigable waters. The authority for these "navigable waters" has been delegated to two primary agencies: the Coast Guard and the Army Corps of Engineers (Sherman, 2002). Other national-level agencies involved in maritime trade issues include U.S. Customs and Border Patrol (CBP), the Federal Bureau of Investigation (FBI), and the U.S. Maritime Administration (MARAD).

Thus, before September 11, we see political agents and agencies in control of the port authority; private actors as owners of terminals; and the Coast Guard as the ultimate guardians of safety and security. However, even this list does not fully articulate the full range of stakeholders that participate in a port's operations. For instance, privately-owned custom brokers have also evolved to intermediate between the government's customs agencies and the importers/exporters that are shipping goods through a seaport. These organizations can expedite goods through customs but in recent years, CBP has been more aggressive in assessing penalties against customs brokers for allegedly "failing to exercise responsible supervision and control" (Customs Brokers, 2014). In one particular case in 2012, the CBP officials charged 3 companies with illegally importing hundreds of millions of dollars in foreign goods into the U.S. (U.S. Department of Health and Human Services, Food and Drug Administration, 2012).

Many unions are also part of seaport governance. For instance, the International Longshore and Warehouse Union (ILWU) represented 33,270 union members in the

United States and Canada in a variety of trades (Form, 2015). The International Longshoremen's Association (ILA) represents more than 40,000+ seaport workers on the East and Gulf Coasts of the United States (Form LM-2, 2015). The Seafarers International Union (SIU) is an organization of 13 autonomous labor unions comprising more than 35,000 mariners, fishermen and boatmen working aboard vessels flagged in the United States or Canada (Seafarers, 2015). The International Brotherhood of Boilermakers represents workers throughout the United States and Canada in a wide variety of professions including heavy industry, shipbuilding, manufacturing, railroads, cement, mining, and related industries (Boilermakers, 2015).

Other actors include trade associations that usually charge a fee for membership and serve as an informal (or formal) lobbyist for the collective group of private firms that operate within a port. Depending on the issue and the personalities of its individual staff, some trade associations amass a great deal of power and ability to lobby both the Administration and Congress. Private freight forwarder firms also represent another type of economic actors. These firms are crucial to facilitating cross-border trade as international trade experts "booking vessel space, preparing relevant documentation, paying freight charges, and arranging inland transportation services" (Murphy & Daley, 2001).

The sheer scale of U.S. seaports is vast in its scope. According to the American Association of Port Authorities (AAPA), there are more than 150 deep draft seaports under the jurisdiction of *126* public seaport agencies located along the Atlantic, Pacific, Gulf and Great Lakes coasts, as well as in Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands. (Sherman, 2002). Many of these seaport agencies are governed by

an elected and/or appointed body, such as a port commission. To illustrate how expansive seaports are on the U.S. east coast, for example, Figure 2.3 displays a map of all seaports and terminals located on the east coast of the U.S. Nearly 30 million containers arrive in the United States each year. 11 million arrive by ship, 11 million overland by truck and another 2.7 million by rail (U.S. Customs, 2016). To demonstrate the institutional complexity of seaport governance, two examples of specific seaports are given below.

2.2.1 Hybrid Governance: The Port Authority of New York and New Jersey (PANYNJ)

The Port Authority of New York and New Jersey (PANYNJ) is a joint agency shared between New York and New Jersey. The PANYNJ manages far more than simply seaports, however. PANYNJ "conceives, builds, operates and maintains infrastructure critical to the New York/New Jersey region's trade and transportation network. These facilities include America's busiest airport system, marine terminals and ports, the PATH rail transit system, six tunnels and bridges between New York and New Jersey, the Port Authority Bus Terminal in Manhattan, and the World Trade Center" (Overview, n.d.). Please refer to Figure 2.4 for a PANYNJ facility map.

Governors from both New York and New Jersey appoint six Commissioners each for six year terms on the Board of Directors for the PANYNJ. These Commissioners are considered to be public servants and their actions on the Board may be vetoed by their respective Governor (PANYNJ Governance, n.d.).

The PANYNJ seaport webpage lists 36 affiliated associations on its website, ranging from labor unions to marine underwriters. In addition to more than 100 private sector seaport partners, another 36 municipal, county, state and federal agencies are listed in the PANYNJ Directory including:

- Borough of Brooklyn, President's Office
- Borough of Manhattan - Borough President's Office
- Borough of Staten Island - Borough President's Office
- Bronx Borough President's Office
- City Hall of Elizabeth
- City of Bayonne NJ - Municipal Offices
- City of Newark NJ - Municipal Offices
- County of Essex NJ - County Executive's Office, Joseph N. DiVincenzo, Jr., Essex County Executive
- County of Hudson NJ - County Executive's Office
- Department of Economic and Housing Development, City of Newark
- Empire State Development Corporation
- New Jersey Department of Transportation, Office of Maritime Resources
- NY State Department of Environmental Conservation
- NYC Commission for the United Nations, Consular Corps, and Protocol
- US Department of Agriculture - APHIS- PPQ
- US Department of Commerce/New York US Export Assistance Center
- US Environmental Protection Agency - Region 2
- Customs & Border Protection
- Customs & Border Protection BSC
- Department of Transportation Region 11 Office
- Federal Highway Administration - NJ Division
- Federal Highway Administration - NY Division
- Food & Drug Administration Help Desk
- Maritime Administration
- U.S. Customs and Border Protection - Port of Entry - New York/Newark
- US Census Bureau- New York Regional Office
- U.S. Coast Guard - Sector New York
- US Department of State, US Despatch Agency
- US Export Assistance Center - New York
- US Export Assistance Center - Newark
- US Fish & Wildlife
- USDA Agriculture Marketing Services
- USDA, Aphis-PPQ Propagated Plants and Cold Treated Fruits
- USDA, Aphis-VS Pet Import/Export
- USDA, FSIS Meats & Poultry

The sheer numbers of stakeholders involved in a seaport start to illuminate the many challenges facing seaport governance. The list above does NOT include the myriad of vendors, terminal operators, shippers, labor unions and a host of others.

The PANYNJ manages a large geographic area across two states and leases most of its terminal space to private terminal operators. To understand the scope of these combined operations, the PANYNJ moved 3,342,286 cargo containers in 2014 worth more than $200 billion - resulting in its position as the busiest seaport on the U.S. east coast with 30% of market share. In addition to the leased terminals, the PANYNJ also maintains public berths primarily for vehicle transshipment and breakbulk loading/offloading (PANYNJ About, n.d.).

Interestingly, the PANYNJ does not receive funds from either the New York or New Jersey treasuries. Rather, the PANYNJ is self-funded and develops its budgets, capital acquisitions and finance options from its own business operations and based on its own creditworthiness (PANYNJ Financial, n.d.).

2.2.2 Hybrid Governance: South Carolina Ports Authority

South Carolina Ports Authority (SCPA) oversees two seaports, in Charleston and Georgetown, and an inland port facility, in Greer. Unlike the PANYNJ with its broad reach into intermodal transportation systems, the SCPA is focused on developing and facilitating waterborne commerce. SCPA has a nine-member Board of Directors, appointed by the governor, as well as two *ex-officio* members, the South Carolina secretaries of Commerce and Transportation. "The port facilities are owner-operated terminals, meaning the SCPA owns the terminals, operates all container cranes, manages and operates all container storage yards and leads all customer service functions in both the yard and the lanes" (SC Ports, Missions, n.d.). SCPA is a public agency yet "despite its status as a public agency dedicated to the economic development of the State of South

Carolina, the Ports Authority does not receive direct appropriations from the state for capital or operations expenses. Instead, the Ports Authority operates like a private business, and funds its operations and investment efforts through its own revenue stream and ability to issue bonds" (SC Ports, 2015).

The SCPA owns and operates five marine terminals (three of which are container terminals: North Charleston, Columbus Street, and Wando Welch). The SCPA is developing a new container terminal on the site of the former Naval Base Charleston and is currently watching negotiations with the State of Georgia for the creation of a new Bi-State Jasper County Terminal on the Savannah River (Chambers, 2015). See Figure 2.5 for a map of the Charleston area terminals.

2.3 Research Design

The research objectives were to explore the effects of the September 11th terror attacks on institutional change in seaport governance. While the approach I took to studying change in seaport governance changed over time, as I will discuss in more detail at the end of this chapter, my original empirical questions related to the role of the Transportation Worker Identification Credential (TWIC) as an outcome of the September 11th events.

The TWIC is a multi-billion dollar security program that started with a few words of text in a post-9/11 piece of legislation. Originally intended as a biometric identity card to control and limit access on seaports, the program grew with an intention of being a multi-modal transportation card valid for a variety of transportation sectors beyond the maritime industry. Interestingly, while the same agency that was responsible for developing the card, the newly formed TSA, had nationalized the passenger screening

function at airports, the TSA role at seaports was limited and the only nationalization of security that was to be implemented was the identification credentials themselves.

Thus, a particularly interesting part of studying TWIC related to the introduction of a new type of security actor into the mix of seaport governance: the TSA. Created after 9/11, the TSA is responsible for ensuring the security of transportation security, including mass transit, rail, trucking, intercity buses and a host of other conveyances.

Since the lead role in maritime is the Coast Guard, TSA has focused primarily on passenger security and intermodal connectivity to ports. As this study indicates, TSA was also tasked with creating a biometric identification credential for seaport access, identified as TWIC. Thus, the study of TWIC did not relate solely to the introduction of new rules about who was allowed on a seaport, but also a directly attempted to introduce a new type of security agent into the already complex mix of actors of seaports. Thus, the case represents a unique experiment to look at the introduction of an ideal type security logics of protecting seaports into a complex institutional setting already attempting to coordinate multiple logics and actors across the political, economic and security sectors.

Below are the original research questions designed to examine the roll-out of the TWIC program:

1. Which stakeholders influenced the roll-out of the TWIC program and led to changes with its eventual implementation over the 12-year period following 9/11? How did the stakeholders influence the implementation of the TWIC program? What are the relationships between stakeholders and how did these relationships affect the eventual program implementation and thus the business environment?

2. What historical influences shaped the position of various stakeholders? What was the rationale for the various stakeholders' positions and how did these positions manifest themselves?

3. Are there particular differences in the histories, trajectories and influences of the various stakeholders (including geographic, proximity to transnational terror incident, local cultural biases, etc…) between stakeholders in New York and Charleston and what does this tell us about how national security policy affects the business environment both on the national and the local level?

4. Was time a factor in determining the strength of stakeholders' positions as the tragic events of 9/11 grew increasingly distant?

2.4 Interview Protocol

I conducted open-ended interviews encouraging the interviewee to explain the position of his or her representative organization with respect to institutional outcome implementation. All recorded interviews took place either at the interviewees' workplace (in person, Skype or telephone) or at their home (Skype or telephone). Always with the permission of the interviewee, I used a voice recording device with permission of the interviewee to capture the conversation. Many interviewees did not give me permission to record either electronically or on paper. Those interviews were strictly "off-the-record" and were not used as part of this dissertation but still served a useful role in providing insights as to where to turn next.

The original sample interview protocol included the following questions:

- What was the original position of your organization with respect to the TWIC program?
- How did your organization make this position known?
- Which organizations did you organization see as "allies" in terms of the position you mentioned?
- What interaction did your organization have with other stakeholders?
- Who did your organization see as the primary stakeholders for the TWIC issue?
- What impact has the TWIC program had on the business environment?
- Is the TWIC related to the events of 9/11?
- How does your organization generally approach security directives from the national government? For firms: does your firm consider security implementation to be an investment or an expense?

- How as the TWIC program evolved since its inception and what has been the role of your organization throughout that evolution?
- Are there other types of directives other than security that your organization receives from the national government and must then decide how to implement?
- If so, how does your organization historically approach these types of directives?

The research proposal was approved and the Institutional Review Board (IRB) made a determination that the proposed activity was exempt from the Protection of Human Subjects Regulations since the primary subjects of our inquiry were on the organizations and institutions rather than the individual people.

The participants were told that their identities would be kept confidential throughout the process of data collection as well as in the analysis and write-up of the study findings unless they gave permission otherwise. Every effort has been made to ensure that participants cannot be identified in the final written products of the study. One difficulty with this type of terrorism-related data collection is that many of the security officials that were willing to discuss security with me only do so on the condition of anonymity. However, personal relationships developed over a lifetime of professional interaction enabled me unique access to many current and former high-level officials. One of the primary challenges mentioned in the academic literature is the real difficulty researchers have in the field of security gaining access to the knowledge and data required of academic study (Suder & Czinkota, 2013). I was able to overcome this barrier. In that regard, doing so required a degree of professional courtesy that in many cases amounted to ensuring anonymity of sources. Not all sources asked for complete anonymity but the percentage was very high and a condition of interviewing in many circumstances.

As it was, I asked interviewees for oral histories on the relationship of their organization and essentially the effectiveness of federal and state regulators. In addition, considering the relationship and method of developing their organizations' position with respect to institutional outcomes and implementation might have divulged internal business practices or relationships that may be harmful to either the interviewee's reputation or the organization that they represent. Particularly when we talk about security-related issues in any form, many people are very reluctant (rightfully so) to discuss security in a public forum. Thus, disclosing the type of information that will help me truly understand the relationship between stakeholders and the manner with which stakeholders approached the TWIC program, for example, was crucial for the success of this research.

It is important to note that I did not include any classified material in this written dissertation. This is an *unclassified* dissertation.

2.4.1 Interviews

The interviewees were representatives of the various key stakeholder organizations involved with the implementation of the institutional outcomes in the twelve years after 9/11. I initially reached out to my existing network of security professionals for referrals of potential interviewees. Oral history interviewees were then selected – sometimes chosen by their own organization and sometimes by me. I originally intended to interview at least 30 people. This sample size should have proved adequate to more fully understand the oral history of the various stakeholders involved with institutional outcome implementation. As it turns out, I conducted 46 recorded

conversations and another 30 that were not recorded but served primarily as background. There was no compensation awarded for interviews. See Appendix B for a complete list of subject matter expert interviewees. After all interviews, I sought primary sources supporting documentation for the facts that they provided and I was sure to ask each interviewee for any supporting information.

2.5 Grounded Theory: The Emergence of Area Maritime Security Committees and Area Maritime Security Plans

As the review of the existing literature suggests, there are few existing theoretical frameworks to guide research into the institutional effects of a transnational terrorist event. In the absence of a large gap of theoretical work to understand an important social and economic phenomenon, I chose to engage in a grounded research methodology. Grounded theory successfully marries theory and research through a systematic process of discovery. The analytic approach can "produce a robust and astute hypothesis grounded in research" (Glaser & Strauss,1967; Strauss & Corbin, 1990; Glauser, 1992; Strauss & Corbin, 1998; Kenny & Fourie, 2014). Essentially, grounded theory involves the use of an intensive, open-ended and iterative process that simultaneously involves data collection, coding (data analysis) and memo-writing (theory building) (Groat & Wang, 2002).

Thus, I realized that Burgelman's (2011) description of the research activities associated with the core of grounded theorizing were ideal for accessing the type of security data that heretofore had eluded researchers and limited inquiry into the long term effects of terror events on the business environment. This research activity became a roadmap for the study: identifying a social phenomenon and starting data collection;

constantly comparing data about different instances of the phenomenon (both success and failure cases where appropriate); in the process of comparing, continuously coding the data to arrive at novel categories and their properties by way of writing brief memos that serve conceptualization; letting the emerging theoretical insights into these categories determine the search for additional instances of the phenomenon (theoretical sampling); and continuing the sampling process (again, both success and failure cases where appropriate) until additional instances no longer add further insight (saturation). Field notes and conceptual memos form the basis for generating the grounded theory about the phenomenon under investigation" (Burgelman, 2011). The fact that such methods could help "understand key aspects of complex social processes captured in historical narratives, while also providing stepping stones toward the development of better grounded, [theory]" was very compelling (Birkinshaw, Brannen & Tung, 2011).

While I started the dissertation to explore the role of TSA in the introduction of TWIC, the interview process led me to expand the scope of my research to include a second comparative case: the role of Area Maritime Security Committees (AMSCs) in implementing new Facility Security Plans (FSP) following 9/11. If TWIC attempted to set the rule about who was allowed on the seaport, the FSPs emerged as an effort to define which areas were security-sensitive on ports, who would be allowed to access those areas, and who should enforce entry into those areas.

Then, grounded theory development altered the course once again. As the systematic categorization of information collected, positioned within the theoretical institutional logics models and the outlines of the interconnected story began to come into focus, I had felt like the FSPs were the real success story under the AMSCs. However,

reviewing the interviews, reading more from primary source documents, and reconsidering the theoretical implications, I realized that the Area Maritime Security Plans (AMSPs) were the real story here. Thus, I came to the conclusion that in addition to the TWIC program, a comparative analysis of the processes and governance structures associated with development of the AMSPs were an important piece. Just as the TSA was a new actor after 9/11, so too were the AMSCs. The parallelism between the TWIC and the AMSP processes began to show large variation in their implementation strategies, progression of institutional logics salience and their overall approach.

Once in focus, this story continued to unfold. The AMSC evolved to include other programs under its purview which are disclosed in the following post-9/11 based case study.

Most interesting for the theoretical topic of my research for looking at institutional change processes following terrorist events, the implementation of the AMSPs took place through a completely different process of institutional hybridity than the TWIC card implementation. The institutional strategy in TWIC was designed to what the theoretical literature called a "replacement" strategy. In the institutional logics literature, a replacement strategy are considered transformational changes in field level logics and occur when one institutional logics is literally replaced with an alternative logic (Thornton, Ocasio & Lounsbury, 2012).

In contrast, the security plans were designed much more closely with a "hybrid" approach. An emerging theory in the institutional logics literature, hybridization "differs from blending in that the goals of incompatible logics are integrated as complementary;

they do not merely exist" (York, Hargrave & Pacheco, 2016). It is this hybridization of security and market logics that leads to sustainable security programs in the long run. Thus, as in any grounded theory research that allows for a constant reiteration between theory and empirical focus (Glaser, Barney & Strauss, 1967), I added a comparison case to the study of the TWIC as one avenue of institutional change following September 11th. I compare this to the emergence of AMSPs as well, particularly looking at AMSCs as a comparative case study. To provide fuller background to this alternative case study, I describe below the emergence of these committee structures before September 11th in order to more fully present both cases in the subsequent presentation of my data.

2.5.1 Area Maritime Security Committees

Since AMSCs were formed after 9/11, the following brief discussion will simply showcase their evolution up to that date. Pursuant to its *Marine Safety* mission, the Coast Guard began facilitating public-private partnerships in our nations' seaports decades ago and formalized the marine safety committees in the early 1990s. Marine safety has a specific meaning in this context and is similar today to what it was prior to 9/11. That is, marine safety generally pertains to the safe operation of vessels and port facilities to promote and ensure the safety of life, property and the environment.

Harbor Safety Committees now appear under different names, such as Port Safety Forums, Marine Advisory Associations, Port Advisory Groups or other similar names. Designed to ensure better communications among all stakeholders within the port, these public private partnerships are "defined in the broadest sense as a local port coordinating body whose responsibilities include recommending actions to improve the safety and

efficiency of a port or waterway" (U.S. Coast Guard, Waterways Management Directorate, 2008). Prior to 9/11, local Harbor Safety Committees had involved as an effective forum available to operators and other seaport stakeholders to "organize in a comprehensive way to address and resolve issues that affect port operations" (U.S. Coast Guard, Waterways Management Directorate, 2008).

The participants within these forerunners to the AMSCs are fairly consistent across all port areas and include most of these entities:

- Port Authorities.
- Vessel owners and operators (tankers, dry cargo, barges, ferries).
- Harbor pilots and pilot associations.
- Marine Exchanges.
- Docking pilots / tug and tow operators.
- Shipping agents.
- Terminal operators.
- Industry associations (national, state, and local).
- Organized Labor.
- Commercial Fishing Industry Associations.
- State / Local Government agencies:
    - Environmental Agencies.
    - Maritime Administrations.
    - Regional Development Agencies.
    - Emergency Management Agencies.
    - LEPC (fire and police departments, harbor masters).
- Federal Government representatives:
    - U.S. Coast Guard.
    - National Oceanographic and Atmospheric Administration (NOAA) -- Hydrographic group.
    - U.S. Army Corps of Engineers (USACE).

(U.S. Coast Guard, Waterways Management Directorate, 2008)

In 1999 and 2000, the Interagency Commission on Crime and Security in U.S. Seaports made recommendations that the Coast Guard take the lead in creating security committees developed along similar lines to the Harbor Security Committees. Several bills were drafted and submitted in 2000 including S.2965 Port and Maritime Security

Act of 2000 sponsored by Senator Ernest Hollings (D-SC) which required the Coast Guard to "establish seaport security committees… [and] implement port security threat assessments… implement security guidelines" (Hollings, 2000). Needless to say, this proposed legislation died in committee until it was suddenly revived and given new life as we shall see in the case study.

2.5.2 Area Maritime Security Plans

One additional pre-9/11 proposal that fell short of its intended goal was a national push for seaport security plans. On July 27, 2000, more than one year before the tragedy of 9/11, Senators Graham and Hollings stood on the floor of the U.S. Senate to introduce their Port and Maritime Security Act of 2000. They began by reporting on the Interagency Commission on Crime and *Security* in U.S. Seaports [emphasis added]. The Commission had issued preliminary findings about the myriad of problems it had found throughout seaports in the United States, Rotterdam and Felixstowe (largest container seaport in the United Kingdom). The senators went on to enumerate key security problems discovered at U.S. seaports including the fact that ports did not conduct vulnerability assessments and thus had no idea what threats they were actually facing noting that what vulnerability assessments were done were not "performed locally." They went on to state, "a lack of minimum security standards at ports and at terminals, warehouses, and trucking firms leaves any ports and port users vulnerable to theft, pilferage, and unauthorized access by criminals" (Interagency Commission, 2000). Perhaps not surprisingly in the summer of 2000, the Commission on Crime and Security at Seaports had relatively little focus on international terrorism compared to what the events 14 months later would bring about for years thereafter.

Nevertheless, the Senators continued speaking about their proposed bill calling upon the U.S. Coast Guard to establish local port security committees at each U.S. seaport with membership to include local port authority representation as well as labor organizations, private sector, federal, state, and local government officials and that the committee would be chaired by the local U.S. Coast Guard Captain of the Port. The bill went on to require creation of a Task Force on Port Security to develop a system of assessing seaport threats and "to create local port security committees to participate in the formulation of these security guidelines" (Graham, 2000).

The Port and Maritime Security Act of 2000 died in committee and never was implemented in its original form. However, as the case study unveils, it was reborn with laudable results.

2.6 Conclusion

As the grounded study progressed, I considered various formats on how to present the results. I chose an historical narrative approach rather than a simple description. This is a story about the complexity of critical infrastructure (in this case, seaports) and the entry of new actors. It is not just a story about changing old rules as a result of the terror attack but more importantly about the new players introduced after 9/11 and the resultant changes in governance structure that led to both success and failure of sustainable security-related programs. From a theoretical perspective, we are able to see the dominant logics employed by each set of actors and we trace the historical progression of these logics as the boundary conditions evolved and eventually give way

to a comparative case analysis between TSA and the TWIC process on one hand and the AMSC and its security plans on the other.

Thus, what follows is the systematic progression of my research presented in a chronological format. Ever mindful of Gaddis' warning to historians that "another of the polarities involved in historical consciousness: the tension between the literal and the abstract, between the detailed depiction of what lies at some point in the past, on the one hand, and the sweeping sketch of what extends over long stretches of it, on the other" (Gaddis, 2002). I did not attempt to trace every precise detail of every minute over the course of 10 years of post-9/11 security-related policy, laws and decisions. However, I feel confident that the following case study contains most of the key events associated with seaport security and the evolution of both the TWIC and the AMSC processes.

There was a clear distinction between the actions of actors before and after 9/11. I initially divided the decade after 9/11 as one in which the security logics likely held primacy immediately after the attacks but which gave way eventually to the primacy of the market logics. What I discovered and what the reader will find next is that this breakdown had to be modified to better understand the role that the DPW case had with its temporary salience of the political logics. Thus, three periods of time are presented corresponding with the evolution of post-9/11 institutional logics that I determined to be dominant.

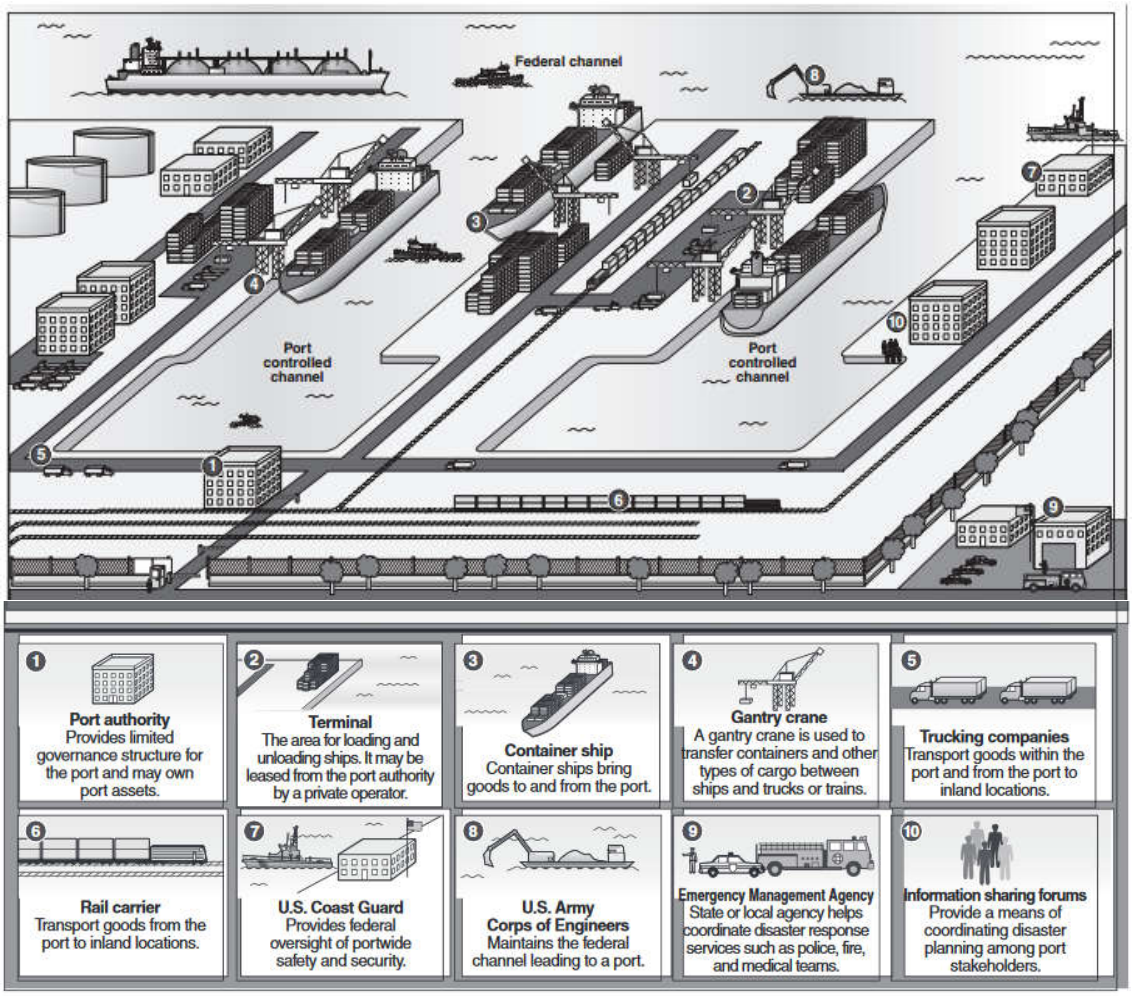


FIGURE 2.1: GRAPHICAL DEPICTION, VARIOUS SEAPORT STAKEHOLDERS

Source: Government Accountability Office, 2011.

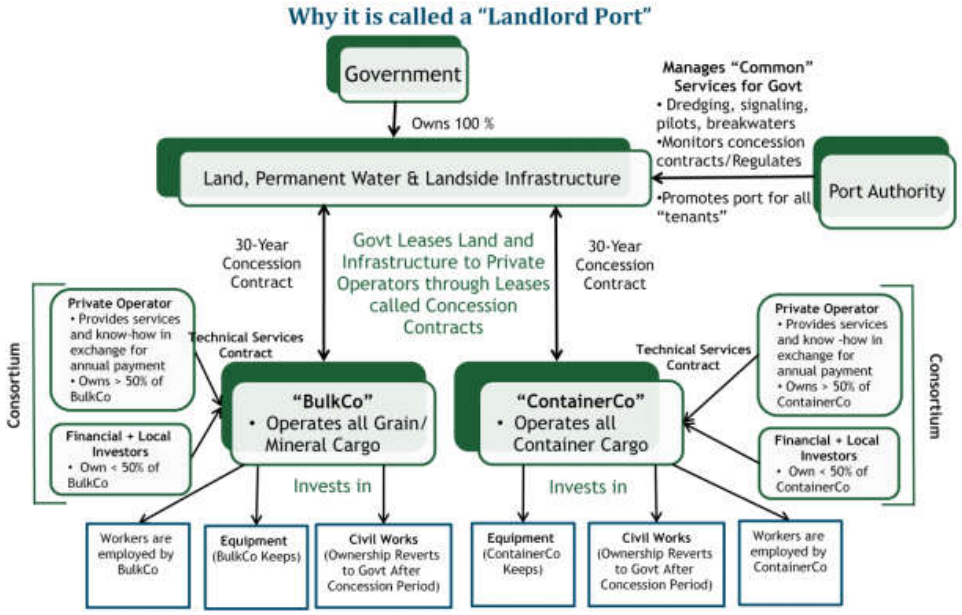


FIGURE 2.2: LANDLORD PORT DEPICTION

Source: The World Bank, Public-private-partnership in infrastructure resource center. (n.d.).

FIGURE 2.3: MAP OF U.S. EAST COAST PORTS AND TERMINALS

Source: U.S. Dept. of Transportation, Bureau of Transportation Statistics

FIGURE 2.4: PORT AUTHORITY OF NEW YORK AND NEW JERSEY FACILITY MAP

Source: Port Authority of New York and New Jersey, Overview, 2015

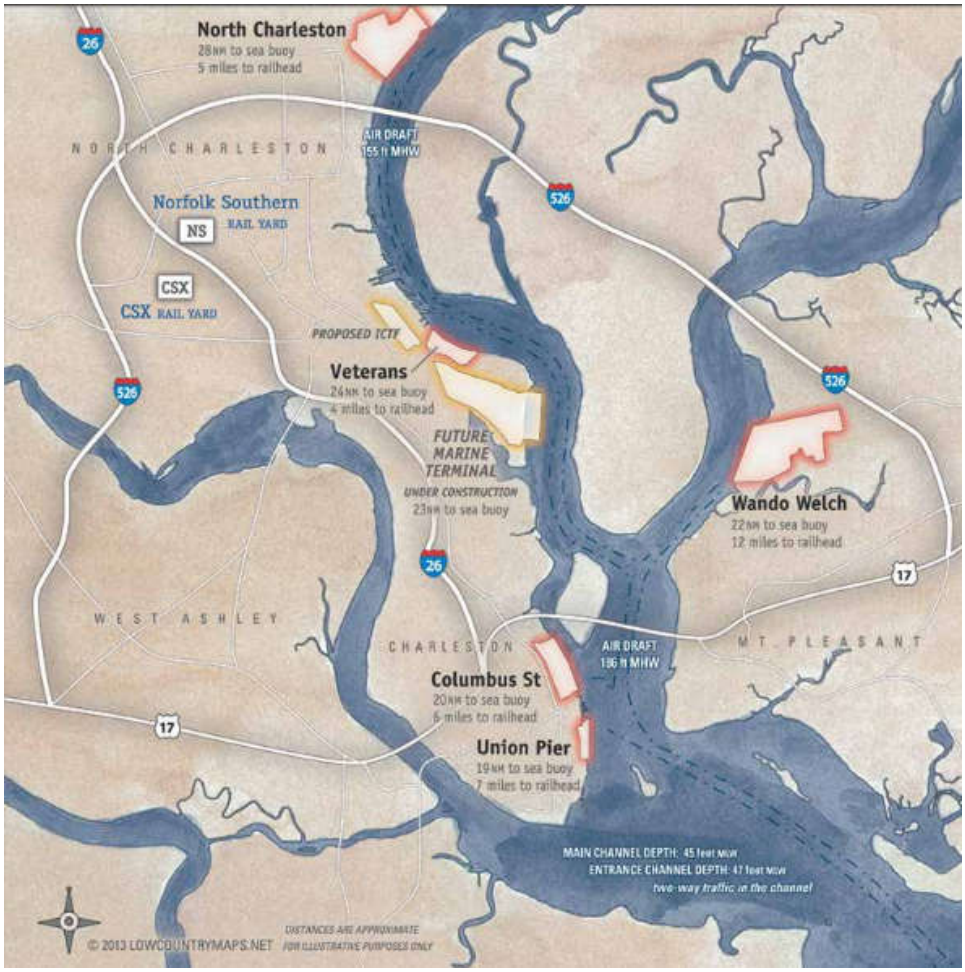


FIGURE 2.5: MAP OF CHARLESTON SEAPORT

Source: South Carolina Port Authority, 2015.

CHAPTER 3: SHAPING THE PUBLIC-PRIVATE BOUNDARIES OF INTERNATIONAL SEAPORT GOVERNANCE AND ACCESS

"Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts. The victims were in airplanes or in their offices: secretaries, business men and women, military and federal workers, moms and dads, friends and neighbors. Thousands of lives were suddenly ended by evil, despicable acts of terror. The pictures of airplanes flying into buildings, fires burning, huge structures collapsing have filled us with disbelief, terrible sadness and a quiet, unyielding anger. These acts of mass murder were intended to frighten our nation into chaos and retreat. But they have failed. Our country is strong. A great people has been moved to defend a great nation."- U.S. President George W. Bush, Address to the Nation, 11 September 2001.

3.1 INTRODUCTION

With smoke in the air, fires still burned at the former World Trade Center site in New York, at the Pentagon outside Washington, D.C., and in a farmer's field in rural Pennsylvania. The trauma of the day's events was played continuously across the cable news channels. Airplanes flying into buildings… huge structures collapsing… estimated death tolls in the tens of thousands even… it was a day that inflicted trauma on the world. With airspace closed and seaports on maximum security alert, global trade in so much as the U.S. portion of was concerned, had ground to a near halt. International stock markets were closed and the world seemed to wait to see what else would follow.

This case study begins after the punctuated international terror attacks on September 11, 2001. It follows the three primary logics employed by the actors associated with the long-term public and private sector actions and the institutional change driven by the interaction of those logics. The actors are important in this story in that through their negotiated and contested collective actions, we are able to study the long-term effects of terrorist attacks on security-related institutional change. My analysis is designed to explore the changing security-related rules in the business environment following 9/11, and just as importantly, the introduction of new types of security actors into the overall governance of seaports.

Central to this narrative is the development of two different security initiatives over the decade following 9/11: The Transportation Worker Identification Credential (TWIC) and the Area Maritime Security Plans (AMSP). Two new types of security actors, the Transportation Security Administration (TSA) and the Area Maritime Security Committees (AMSC), both drew their mandate to implement the TWIC and AMSPs, respectively, from the same piece of legislation. The Maritime Transportation and Security Act of 2002 was the genesis for both programs. However, shifting security logics and implementation over the same time period and with roughly the same actors and externalities resulted in significant variance both in terms of benefits and sustainability of the security programs with respect to their original intent. This is a fascinating study of the long term effects of terrorism on the business environment due to several contributions including the introduction of a new security logic, exploration of the multiple logics' interactions resulting in intuitional change, and the lessons to be potentially garnered from all of this for future security strategy.

As far as 9/11 is concerned, this study will not provide a detailed description of that fateful date. Suffice to say, the single best source of inquiry into the events and actors from that tragedy remains the painstakingly crafted 9/11 Commission Report (National Commission, 2004). Instead, I turn to a recommendation from the 9/11 Commission Report that, "[h]ard choices must be made in allocating limited resources… [We] 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 should assign roles and missions to the relevant authorities… and to private stakeholders. In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure" (National Commission, 2004). The actual details of how such a broad mandate is actually implemented in practice sets the stage for this close analysis of changes in seaport governance in the decade following 9/11.

3.2 Act I: 2001 to 2004: The Growing Salience of Critical Infrastructure Security

"It is my hope that in the months and years ahead, life will return almost to normal. We'll go back to our lives and routines, and that is good." - President George W. Bush, Address to a Joint Session of Congress, September 20, 2001 (Bush, 2001)

What President Bush seems to have foreseen when he made this address to the nation is that the events of 9/11 had created a "new normal." Nothing would be exactly the same as it was pre-9/11. However, security was not a new phenomenon on September 12, 2001. It had obviously been a concern long before 9/11. Various Presidential Directives in 1982, 1985, 1986, 1995, 1998, and 1999 had specifically dealt with counter-terrorism efforts and the private sector maintained security forces, secure

areas and other forms of protection. Nonetheless, many of these efforts were limited in scope, uncoordinated and/or only addressed limited aspects of terrorism (*e.g.*, plane hijackings). For the most part, security, particularly at seaports, focused on the internal threat of theft and pilferage rather than an external threat. Likewise, inspections and law enforcement were more concerned with importing counterfeit products and smuggling narcotics more so than terrorism. Thus, in the immediate aftermath of 9/11, both public and private sectors scrambled to define new strategies for protecting critical infrastructure (*e.g.,* airports, seaports) in light of the growing security logics dominance.

A portion of the U.S. Government assumed a war footing in the immediate aftermath of 9/11. In a televised speech to the American public, President Bush warned, "Every nation, in every region, now has a decision to make: Either you are with us, or you are with the terrorists" (President, 2001). Separating out this wartime component of the public policy sector's response to 9/11, which included invading Afghanistan and dismantling the Taliban, this study focuses more on the domestic response as it relates to seaport security and the long-term implications for the business environment. These implications have far-reaching implications for firms around the world.

The international response was broad-based and the security logics is evident here as well. The United Nations held an emergency meeting of the Security Council on September 12, 2001, resulting in a unanimous resolution which "*Unequivocally condemns* in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington (D.C.) and Pennsylvania and *regards* such acts, like any act of international terrorism, as a threat to international peace and security" (United, 2002). Within days, multiple nations had passed resolutions condemning the

attacks and stating their belief that 9/11 was considered to be an attack on all nations. These international responses included the Organization of the American States (OAS), North Atlantic Treaty Organization (NATO) and the Australia-New Zealand-United States (ANZUS) pact (U.S., 2001). While initial focus might have been on aviation security, maritime security presented particular challenges for the global economy.

Testimony to Congress by both public and private officials has explained on numerous occasions why seaport security was a viable concern for the economy. A Port of Los Angeles official told Congress of a 2002 labor dispute that cost the economy nearly $1.5 billion per day with the Government Accounting Office (GAO) adding that a "terrorist attack at a port facility could have a similar or greater impact" (Government Accounting Office, 2009). "[Seaport]…systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas. A terrorist attack on these systems and facilities could cause a tremendous loss of life and disruption to our society. An attack would also be costly" (Government Accounting Office, 2009).

The story told in this first time period (2001 to 2004) revolves around the rise of security logics as a determinant of actions by the political/public policy actors, the security actors and the economic actors. This leads to the formation of new organizational forms to implement the security logics on behalf of the political/public policy actors. However, outside of airports where the TSA and the politicians moved quickly, this initial period did not provide many concrete details about what actions should be taken by private sector actors in the seaport sector. As a result, for immediate

solutions, security actors turned to existing ideas and legislation that had not been implemented prior to 9/11. Thus emerged programs such as the TWIC and the AMSPs.

3.2.1 The Emergence of New Security Focused Actors

The most lasting impacts of 9/11 were major public sector governance changes designed to identify and defend the security of the country from future attacks. The government proposed, and subsequently adopted, the largest government reorganization since the National Security Act of 1947 created the National Security Council and the Department of Defense. Almost immediately, Congress passed numerous pieces of legislation as a short-term response to 9/11, including giving the President the power to use "all necessary and appropriate force" to strengthen the ability of security agents to combat terrorism (Joint, 2001). Among a host of other laws passed were the: United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, the Aviation and Transportation Security Act of 2001, and the Maritime Transportation Security Act (MTSA) of 2002.

One of the first visible signs of structural governance changes came within days of the terror attack: the creation of a White House Office of Homeland Security, led by former Pennsylvania Governor Tom Ridge, and the Homeland Security Council. At an initial press conference naming several senior appointees to the newly established organization, National Security Advisor Condoleeza Rice said, "[w]e commonly hear the refrain that everything changed on September 11th. In many ways, that is true. And one of the things that has changed is how we are going to organize the United States government to defend against, and ultimately defeat, the threat of terrorism" (Rice, 2001).

The governance structure decided upon was centralized control and the amalgamation of twenty two separate agencies under the Department of Homeland Security fewer than 2 years later in 2003.

In addition, pursuant to the November 2001 Aviation and Transportation Security Act (ATSA), a new agency, the TSA, was specifically given the responsibility to protect the security integration of the U.S. transportation system. Pursuant to its name, the TSA was intended to provide a comprehensive transportation security role. The TSA's initial mission was dedicated specifically to the public regaining confidence in the national aviation system including nationalization of passenger and baggage screening[4] at over 440 commercial airports in the United States by November 19, 2002, and the screening of all checked baggage using explosive detection systems (Aviation, 2001). With little time for strategic planning, the fledgling agency quickly found itself with a two-fold challenge of addressing the typical bureaucratic hurdles associated with standing up a new agency while at the same time hiring more than 60,000 airport screeners for the purpose of nationalizing airport security screening. By mid-2004, TSA still had not hired enough screeners to fully staff screening checkpoints "without using additional measures such as mandatory overtime" (Rabkin, 2004).

There were early signs of concern for related security issues within seaports, but there was significantly less substance of what this meant in practice, particularly in relationship to the responsibilities of the new security agencies in relation to the Coast Guard (which traditionally held primary responsibilities for seaport security). The

[4] Interestingly, in 2004 TSA created the Screening Partnership Program (SPP), allowing TSA-regulated airports to apply to have screening of passengers and property performed by private contractors rather than TSA.

Marine Transportation and Security Act of 2002 (MTSA) contained provisions for several seaport security initiatives including a small provision regarding biometric port access and the implementation of vessel and facility vulnerability assessments and subsequent development of security plans to be approved by Coast Guard Captain of the Ports (COTP). Likewise, the MTSA required the creation of AMSCs at all major ports to coordinate and foster public private partnerships, whose purpose was development of the first comprehensive maritime security assessments and plans.

The National Strategy for Combating Terrorism released in 2003 had no specific mention of seaports but did allude to the need to maintain maritime domain awareness and a focus on critical infrastructure. "In many cases, U.S. enterprises overseas are linked or networked to domestic critical infrastructure, and a terrorist event overseas would have a cascading effect on domestic reliability. To reduce this possibility, the Department of State will take the lead and, in conjunction with appropriate agencies, identify and prioritize critical infrastructure overseas and partner with industry to establish cost-effective best practices and standards to maximize security" (National Strategy for Combating Terrorism, 2003). This is one of the first instances of the public sector suggesting an expanded security role at the intersection of the public and private goals in protecting critical infrastructure from terrorist attacks.

In October 2003, the Department of Homeland Security announced its initial promulgation of maritime industry security rules designed to improve security for seaports, waterways and ships. The strategy articulated a broad vision but provided few concrete details, suggesting that the federal government held three primary responsibilities in regard to protecting seaport security:

(1) to produce and distribute timely and accurate threat advisory and alert information and appropriate protective measures to State, local, and tribal governments and the private sector via a dedicated homeland security information network;

(2) provide guidance and standards for reducing vulnerabilities; and

(3) provide active, layered, and scalable security presence to protect from and deter attacks." (U.S. Department of Homeland Security, National Plan, 2005)

The White House's National Security Presidential Directive (NSPD) 41 / Homeland Security Presidential Directive (HSPD) 13 also focused attention on maritime security. The Directive recognizes "that maritime security policies are most effective when the strategic importance of international trade, economic cooperation and the free flow of commerce are considered appropriately" (White House NSPD41/HSPD13, 2004). The Directive required that the departments of Homeland Security and Defense coordinate a National Strategy for Maritime Security that included "private components" and a concerted effort to outreach to both international and private sector stakeholders for "an improved global maritime security framework" (White House NSPD41/HSPD13, 2004).

This growing discussion of critical infrastructure as a public good that required both public and private participation represented a growing central arena of debate over what exactly should be done, by whom and at what costs. For instance, on June 10, 2003, Coast Guard Rear Admiral Hereth told attendees of an Independent Liquid Terminals Association conference that "the economic impact of any added security is a main concern… The main mission of tightening security along U.S. waterways is to catch the 'bad guys,' but also to minimize the financial impact on companies operating in U.S. ports" (USCG Port Plan, 2003). He estimated "costs to private enterprises could total $1.4 billion in the first year of the act, but added that the costs of a terrorist attack could

have much deeper economic impact… Usually, it's regulator versus regulatee… [but] We try to suggest that it's all of us in this room against the bad guys" (USCG Port Plan, 2003). His discussion of regulators and regulatees provided an early frame of the challenges of introducing new security logics into the overall governance of seaports.

3.2.2 Redefining Public-Private Security Responsibilities

The relative responsibilities of the emergent security-oriented public actors and existing private actors in protecting the collective good of seaport security were explicitly raised in these initial strategy documents but not fully resolved. For instance, the 2002 National Strategy for Homeland Security sheds light on this security logics and its take on private sector incentivization of security expenditures. "Private businesses and individuals have incentives to take on expenditures to protect property and reduce liability that contribute to homeland security. Owners of buildings have a significant stake in ensuring that their buildings are structurally sound, properly maintained, and safe for occupants… Properly functioning insurance markets should provide the private sector with economic incentives to mitigate risks. Costs of homeland security in the private sector are borne by both the owners of businesses in the form of lower income and their customers in the form of higher prices" (White House, Office of Homeland Security, 2002). Subsequently, it reads, "responsibility of providing homeland security is shared between federal, state and local governments, and the private sector. In many cases, sufficient incentives exist in the private market to supply protection. Government should fund only those homeland security activities that are not supplied, or are inadequately supplied, in the market" (White House, Office of Homeland Security, 2002). Seaports

are mentioned in passing but as a means of possible conveyance by terrorists transporting weapons of mass destruction more so than targets in and of themselves.

This discussion of who was to bear the cost of the eventual implementation of new security-related initiatives was also discussed during an August 2002 port security congressional hearing. For instance, the U.S. Director of Physical Infrastructure Issues explained the "conflicting views of the many stakeholders that are involved in port decisions, including government agencies at the federal, state and local levels and thousands of private sector companies… while broad popular support exists for greater safety, this task is a difficult one because the nation relies heavily on a free and expeditious flow of goods. To the extent that better security impinges on this economic vitality, it represents a real cost to the system" (Hecker, 2002). Therefore, we see the conflict between security and market logics from the very outset: the juxtaposition of a willingness on behalf of the private sector to support increased counter-terrorism initiatives after 9/11 on the one side but concern about the impact of those same programs on their competitiveness on the other.

Around the same time, the MTSA initiated a series of port security grant programs overseen by the Maritime Administration (MARAD). A June 12, 2003, Department of Homeland Security press release announced the $170 million in new port security grants and $58 million in funding for Operation Safe Commerce. This accompanied another $75 million for port security grants from the Office for Domestic Preparedness and the $92 million already awarded in the 2002 round of grants (Protecting, 2003). Whereas seaports had received little or no funding for security prior

to 9/11, hundreds of millions began to flow into various projects (some actually related to security).

The private sector recognized the financial windfall this represented and dutifully applied (and received) a large portion of these grant monies. However, when these grant programs were assessed by the Department of Homeland Security Office of Inspector General (OIG) in late 2004, the OIG found "the program's strategic impact is less apparent and its purpose and goals require refinement to support national priorities effectively" (U.S. Department of Homeland Security, Office of Inspector General, 2005). The OIG went on to write that the "question of where the private sector's responsibility for preventing terrorism ends and where the federal government's responsibility begins poses a dilemma for the Port Security Grant Program. The Department of Homeland Security does not have a formal policy to provide financial assistance to private entities, a group that includes those that own and operate high risk facilities. Private entities have applied for and received substantial funding. Some of that funding went to projects that reviewers scored below average or worse during the evaluation process" (U.S. Department of Homeland Security, Office of Inspector General, 2005). Thus, by mid-2004, Homeland Security's own Inspector General stated no coherent understanding of the boundary conditions between the public and private sector was available despite the private sector having received tens of millions in security-related grants.

One of the first private sector seaport programs after 9/11 came in the form of the Customs-Trade Partnership Against Terrorism (C-TPAT) initiated by U.S. Customs and Border Protection (CBP). Some private companies saw this as a way to improve the overall security of their supply chains by conducting an extensive review and approval

process to receive "trusted shipper" certification from the Department of Homeland Security. In turn, containers from these trusted shippers were given expedited priority upon entry to the U.S. as less attention was focused on them during port inspections. Initial appeals for this program were based partly on corporate social responsibility in light of the 9/11 attacks and the need for counter-terrorism partnerships between the public and private sectors. The program has since expanded to include a host of countries in Mutual Recognition Agreements (MRA).

After some wariness following the initial C-TPAT roll-out, recognizing the market logics of expedited shipping containers, firms such as DHL began recommending C-TPAT to its customers as way to "reduce clearance times for your shipments" (International, 2016). After C-TPAT, the next large initiative involving the private sector was the Container Security Initiative (CSI). Proposed by the reformed CBP, private sector shipping interests found the public sector keen to inspect their containers before their arrival in U.S. seaports. Driven by intelligence and international cooperation, the concept was that seaports could essentially push their spatial boundaries out to the last port of call before being loaded onto a U.S.-bound container ship. Yet again, this exemplifies the security logic's preeminence over the economic logic. Pushing out the boundary created a buffer for U.S. interests but potentially increased the threat at foreign seaports, not to mention the additional costs inherent in the delays associated with screening additional containers.

The private sector was very supportive of receiving federal grant monies at the least. In a December 5, 2002, World Shipping Council endorsement, the Council (representing most international shipping lines) stated support for a number of security

initiatives: "[t]he World Shipping Council strongly supports the [U.S.] federal government's efforts to enhance security for the movement of cargo through the international supply chains that serve American consumers and businesses. The Council and its Member liner shipping companies have supported the Customs Service's Trade Partnership Against Terrorism program (C-TPAT), and every Council member has applied to participate in that program. The Council and its Member lines have supported the government's Container Security Initiative and … have strongly supported the U.S. government's successful initiative, led by the Coast Guard, at the International Maritime Organization to establish new international security regime for vessels and marine terminals" (Comments, 2002).

The uncertainty over the role of the private sector played out in many different forms. One criticism that I heard during my interviews was that of the private sector driving security policy in the hope of a financial return in the form of a new program that might employ the services of the firm suggesting it. This group of firms is driven by market logics as well and in the case of this study, is not focused on the seaport or governance so much as they are focused on profiting from the institutional change resulting from 9/11. These interests actually drive security initiatives with pure economic logics rather than security logic.

For example, Oracle CEO Larry Ellison publicly advocated for a biometric, national identification card that his company would be willing to implement. Ellison had meetings with senior administration officials and had outlined a biometric card very similar to what the TSA eventually presented for the TWIC. Industry experts estimated a cost in excess of $3 billion USD: "Ellison said that if he does donate the software,

maintenance and upgrades won't be free. ‘I don't think the government has any trouble paying for the labor associated with the software,’ he said. ‘I made this offer not because the government can't afford to pay for the software, but because I shut up the critics who were saying, `Gee, Larry Ellison wants to build a national database because he wants to sell more databases,' which is pretty cynical and bizarre. What's in it for me is the same thing that's in it for you: a safer America.’” (Ackerman & Rogers, 2001). There are countless other examples of similar security-oriented proposals by companies in position to (1) provide the public sector with real security solutions; and/or (2) make a profit from those same solutions.

Another private sector innovation following 9/11 was the tremendous growth in security-related lobbying firms. For example, the domestic security practice at the Washington law firm of Powell, Goldstein, Frazer & Murphy was led by a lawyer whose online résumé noted that he was the author of a newsletter article titled "Opportunity and Risk: Securing Your Piece of the Homeland Security Pie" (Former, 2003). At Venable LLP, the law firm's 28-member domestic security practice included a former transportation secretary; a former Republican House member from California, and a former general counsel of the Immigration and Naturalization Service. Another illustration of this private sector driven security phenomenon is explained by a Venable LLP partner, “We're trying to help our clients avoid the land mines and find the gold mines in homeland security," said John J. Pavlick Jr., a partner who has helped organize the practice, which represents Lockheed Martin, Raytheon and other large government contractors. "The major defense contractors want to move into the homeland security arena in a big way. I'm very bullish on this" (Former, 2003).

Finally, it is worth noting the "revolving door" of public sector personnel who left military service or other public sector agencies only to be hired immediately by various private sector contractors and sub-contractors providing advice and consulting to the same entities that they had just departed. Thus, individuals with the security logics background suddenly find themselves thrust into the market logic. The effects of September 11th included not just the introduction of new public actors designed to protect security, but also the emergence of new types of economic actors with a financial incentive to focus on related security objectives.

3.2.3 The Emergence of Institutional Experiments

It is within this period of institutional experimentation and uncertainty that I identified the kernel of two concrete security-related initiatives that became the subsequent focus of my case studies: 1) the TWIC and 2) the AMSP. The Maritime Transportation and Security Act of 2002 (MTSA) was the genesis for both programs. As previously stated, the MTSA contained provisions for several security initiatives including a small provision regarding biometric port access. Encompassing fewer than 850 words, this small provision was the beginning of a project spanning over 15 years and hundreds of millions of dollars thus far: the TWIC. In addition, the MTSA required the creation of and the implementation of vessel and facility vulnerability assessments and subsequent development of security plans to be approved by Coast Guard Captain of the Ports (COTP). Moreover, the law called for the creation of AMSCs at all major ports to coordinate and foster public private partnerships whose purpose was development of these comprehensive Maritime Security assessments and plans.

While the initial kernels of these initiatives arose from this early law, the actual implementation of these policies – and the subsequent discussion of the boundaries between public and private responsibility in its implementation – did not fully occur until the DPW scandal began to focus increasing attention of the new security actors onto port Security. The TWIC became governed through the newly-formed TSA, while the development of the security plans were assigned to the Coast Guard and its newly formed cross-sector collaborative organizations, the Area Maritime Security Committees. Thus, these two programs represent distinct institutional experiments about the best way to transform general public concern over the security of ports from terrorism to actual organizational policies that co-exist with existing economic logics and actors.

3.3 Act II: 2005 to 2006, From Airports to Seaports: The Shifting Focus of Security Logics

"The Whole Dubai Ports World fiasco was nothing but a knee-jerk, xenophobic and political 'cherry-picking' by political leaders seeking to bolster their national security platform in a midterm election year." - Arsalam T. Iftikhar, Council on American-Islamic Relations (Iftikhar, 2006)

"National security, not simple economic opportunity, comes first. The Committee on Foreign Investment in the United States (CFIUS) apparently forgot this when it OK'd the deal to shift major port operations to government-controlled Dubai Ports World." - U.S. Rep. Duncan Hunter (Hunter, 2006)

By early 2005, there was a growing sense of "normalcy" within the "new normal." One of the new security-focused actors, the Department of Homeland Security, under Governor Tom Ridge's vision and leadership, had successfully navigated the process of assembling 22 disparate agencies and more than 180,000 employees under a unified command structure with a shared vision and mission. The Department of Homeland Security Office of Private Sector Liaison had taken a lead role in connecting

the private and public sectors with a shared vision of security. Congress was pouring federal money into private sector "security" efforts and maritime trade was growing. And then, political logics shifted the focus of security efforts and suddenly seaport security became a hot topic around the country.

3.3.1 The growing salience of seaport security and resilience following Dubai Ports

In 2006, a political crisis emerged during a mid-year Congressional election that would propel seaport security to the proverbial front burner of national attention. The crisis, precipitated by a routine business transaction in the maritime industry involving Dubai Ports World (DPW), resulted in the most prolonged spotlight on seaport-related counter-terrorism efforts since 9/11 and renewed interested in programs like the TWIC. Following, as it did, on the heels of the CNOOC/Unocal national security case (foreign control of strategic resources) from the year before and the Hurricane Katrina catastrophe - which together had heightened the sensitivity of political logics to security related issues - the DPW deal served to shift the attention of politicians from the post-9/11 focus on aviation to the broader security implications of unsecured seaports.

A May 2005 Congressional Research Service report attempted to justify the various seaport security mandates since 9/11 extolling the many benefits of security enhancements despite the costs. Written by a team led by TSA employees, "[m]any experts see economic benefits to *tighter control over maritime commerce*. Resources put towards seaport security can also reduce cargo theft, narcotic and migrant smuggling, trade law violations, the accidental introduction of invasive species, and the cost of cargo insurance. Improved planning for responding to a terrorist attack at a seaport could also

improve responses to other emergencies, such as natural disasters or transportation accidents. New technologies intended to convert the sea container into a 'smart box,' such as electronic seals, sensors, or tracking devices, could also improve shipment integrity, help carrier s improve their equipment utilization, and help cargo owners track their shipments" (Frittelli, 2005, emphasis added).

On October, 17, 2005, the DPW deal began as a fairly benign application to the Committee on Foreign Investment in the United States (CFIUS). A state-owned company located in the United Arab Emirates, DPW proposed to acquire a British company, the Peninsular and Oriental Steam Navigation Company (P&O) (DP World, 2006). "The P&O Ports terminals DPW would acquire included: Baltimore (2 of 14 terminals at the port), Philadelphia (1 of 5 terminals), Miami (1 of 3), New Orleans (2 of 5), Houston (4 of 12), Newark (1 of 4) and [DPW would be] involved in stevedoring activities at all five terminals in Norfolk. In total, DP World will acquire operations at 11 terminals out of a total of 43 terminals at the six ports, according to DHS" (DP World, 2006).

An initial review by the Coast Guard cited concerns about security. Those concerns included: "[t]here are many intelligence gaps, concerning the potential for DPW or P&O assets to support terrorist operations, that precludes an overall threat assessment…The breadth of the intelligence gaps also infer potential unknown threats against a large number of potential vulnerabilities" (U.S. Senate Homeland Security Committee, 2006). Excluded by later critics of the DPW deal is the fact that the Coast Guard later stated that the concerns reflected in its initial assessment were ultimately addressed. In a statement, the Coast Guard later stated that "[o]ther U.S. intelligence

agencies were able to provide answers to the questions [the U.S. Coast Guard] raised" (U.S. Senate Homeland Security Committee, 2006). After discussing and receiving written assurance from DPW of its willingness to be transparent, the Department of Homeland Security approved its portion of the CFIUS endorsement. On January 17, 2006, the entire CFIUS committee agreed to allow DPW to move forward with its merger.

Suddenly, we see state (political) logics and the "back-room politics" described in the ideal type state logics come into play (Thornton, *et al.,* 2012). A Florida-based firm, Eller and Company, hired a lobbyist to stop the deal. The lobbyist later stated that his client "did not fan anti-Arab sentiment but objected to the DP World deal because the Florida company did not want to be forced into partnership with a company controlled by a foreign government" (Bonney, 2006). And yet, P&O was a foreign owned company.

The lobbyist waited until Congress had returned to session in February 2006 and began his lobbying efforts. Familiar with the Banking Committee, a groundswell of political interest started and then a map of all ports affected by the DPW deal appeared. The epicenter of these initial lobbying efforts was Senator Chuck Schumer (D-NY). Simultaneously, the lobbyist had been speaking with the Associated Press. "In a period of four days, the AP reporter's story ran nationwide, Schumer called for a review by the Department of Homeland Security, and he held a press conference with 9/11 families. He called on President Bush to step in" (Overby, 2006).

What ensued appears to be a direct manifestation of 9/11. One speaker called the Dubai port deal opposition "one of the most cynical campaigns of disinformation and

demagoguery...since Joe McCarthy waved around his phony list of communists in the State Department…driven mostly by emotionalism, ignorance, xenophobia and partisan politics" (Bonney, 2006). Two sides quickly formed under the framework of security logics versus market logics. Nonetheless, the process might better be described as state logics. Concerns were raised about DPW's ties to the UAE and alleged potential ties to terrorism. In February 2006, Senator Chuck Schumer (D-NY) said "[f]oreign control of our ports, which are vital to homeland security, is a risk proposition. Riskier yet is that we are turning it over to a country that has been linked to terrorism previously" (Magnet, 2006).

As the opposition to DPW pointed out, one of the terrorists who flew a plane into the World Trade Center on September 11, 2001, Marwan al-Shehhi, was born in the United Arab Emirates. Other hijackers traveled through that country on their way to perpetrate 9/11 (Magnet, 2006). During a protest rally with seaport union workers in New Jersey, Senator Frank Lautenberg (D-NJ) reportedly said, "'the transfer of title of operations at one of Newark, New Jersey's four terminals constitutes an Arab 'occupation'" (Zunes, 2006) and that "'[w]e wouldn't transfer the title to the devil and we're not going to transfer it to Dubai'" (Friedman & Sherman, 2013).

In a July 2006 review of the CFIUS/DPW event, Larson and Marchik (2006) warned that "the additional strains imposed by the new security challenges following the attacks of September 11, 2001; and the fact that National Security Agreements (NSAs) imposed on foreign companies by CFIUS as a condition for approving a transaction, have placed foreign companies at a competitive disadvantage" (Larson & Marchik, 2006). This review went on to point out the need to balance the security logic, the state logics

and the market logic, saying "[t]here are two fundamental reasons why it is important that Congress and the administration effectively balance the twin objectives of maintaining openness to foreign investment and protecting national security. First, both the economic health of the United States and its long-term security depend on maintaining a welcoming environment for the majority of foreign investments. Second, if the United States creates a restrictive foreign investment climate marked by unnecessarily cumbersome regulatory reviews, other countries will surely follow that course, with real costs to the United States" (Larson & Marchik, 2006).

In the end, DPW did not retain control of the terminals.[5] While all of this transpired, it should be noted that foreign ownership and/or control of U.S. critical infrastructure is not uncommon. In Los Angeles, Chinese, Taiwanese, and Singaporean government-owned companies already operated terminals and "…another Singaporean Government-owned company lost out to Dubai ports in its bid for P&O Ports in the transaction at issue" (Stevens, 2006).

Thus, having weathered Hurricane Katrina, the DPW controversy and emerging reports from both the GAO and the private sector about the failures of TWIC, the public and media began asking what had been done since 9/11 to improve security at seaports. Several of the interviewees for this research stated that at this point, both the administration and Congress were looking for successes in port security. The TWIC

[5] Interestingly, Gulftainer, a privately held, UAE-based terminal operator, unveiled its Port Canaveral, Florida, operation in June 2015 to little fanfare or media coverage. Despite being requested by a Congressman, no Treasury Department Committee on Foreign Investment (CFIUS) review was conducted. According to the port's spokeswoman, the Treasury Department "panel found that no review was required because the agreement was a [35-year] lease and not a purchase of Port assets" (Brinkman, 2015).

program, nearly dead two months earlier, was suddenly targeted as a quick solution to demonstrate port security resolve.

In response, multiple bills were introduced in the U.S. legislature in spring and summer 2006, including one that eventually was signed into law, the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) (SAFE Port Act, 2006). The SAFE Port Act introduced and reinforced multiple port security programs including the TWIC. With little progress on the TWIC to show since the 2002 MTSA, the SAFE Port Act required an implementation schedule for TWICs based on risk and vulnerabilities assessed in earlier regulations. The Secretary of the Department of Homeland Security was mandated to implement TWIC at the 10 top priority ports no later than July 2007 and at all U.S. ports not later than January 2009. The SAFE Port Act also required a pilot program to investigate technical and operational impacts of implementing a transportation security card reader system (SAFE Port Act., 2006).

As previously alluded to, two other events in 2005 also contributed to the growing salience of seaport security. The growing concern of foreign ownership of U.S. assets flared with the Chinese state-owned China National Offshore Oil Corporation's (CNOOC) offer to buy Unocal, a US-owned oil company. A House Resolution dated June 30, 2005 called upon the President to conduct a thorough review of CNOOC's attempt to purchase Unocal Corporation as CNOOC "could take action that would threaten to impair the national security of the United States" (H.R. Res. 344, 109th Cong. 1, 2005).

A second event occurred when Hurricane Katrina struck the U.S. Gulf Coast in August, 2005, with such ferocity that it became the most catastrophic (and costliest) natural disaster in U.S. history. The Department of Homeland Security and many of its associated agencies were criticized for their "Failure of Initiative" as the congressional after-action report would be called. The Federal Lessons Learned report released on February 23, 2006, reaffirmed the role of the private sector: "[c]ompanies are responsible for protecting their systems, which comprise the majority of critical infrastructure. Because of this, private sector preparation and response is vital to mitigating the national impact of disasters. Government actions in response to a disaster can help or hamper private sector efforts. However, governments cannot plan to adequately respond unless the private sector helps them understand what infrastructure truly is critical. Likewise, businesses cannot develop contingency plans without understanding how governments will respond" (The White House, The Federal Response to Hurricane Katrina, 2006). The White House released the Federal Lessons Learned from Hurricane Katrina at the same time a political storm was brewing with the unfolding DPW deal to lead to growing attention to the protection of seaports.

3.3.2 Economic Actors: Adapting to Emerging Rules and Governance Systems

Emerging from this was a clear explanation of the role of the private sector in terms of port security from the perspective of the second highest ranking official at the Department of Homeland Security. During testimony to Congress, Deputy Secretary Michael Jackson testified before Congress about the Role of Terminal Operators (such as P&O and DPW). Deputy Secretary Jackson wrote (and it is worth including here in its entirety):

> Let me first clarify what terminal operators do. They do not run ports. They certainly don't provide or oversee security for the entire port complex. That is the responsibility of the government and the local port authority, which is usually a government agency.
>
> Terminal operators also do not obtain a comprehensive window into the breadth and depth of security measures that DHS employs to protect our ports and the cargo that enters those ports. The public fears that the DPW transaction have generated on this point are misplaced and lack a firm factual foundation, as I will explain later.
>
> Terminal operators ordinarily sign a long-term lease for waterfront property in the port. They build a pier for ships, cranes to unload the ship, a parking lot to store the containers they unload, and perhaps a small management office. They make their money lifting containers out of ships and holding them for shippers.
>
> That's what we're talking about here. Through its acquisition of P&O, DPW is hoping to take over the leases at twenty-four terminals in the U.S. That's a relatively small part of the operations in the six ports where they would operate terminals, including New Orleans, Houston, Miami, Newark, Baltimore, and Philadelphia. Their filings indicate that DPW will also take over the P&O equities at other ports, but these consist of stevedoring and labor operations where P&O is not the designated terminal operator.
>
> I understand from the Coast Guard that there are more than 800 regulated port facilities in the six ports where P&O operates terminals in the U.S. So the twenty-four terminals in question here constitute less than 5% of the facilities in those six ports (Jackson, 2006).

In early March, the Washington Post reported, "[a]dministration officials have asserted in recent days that security at U.S. ports is the responsibility of the Coast Guard and U.S. Customs and Border Protection, with the terminal operators responsible for little more than transferring containers from ships to railroad cars and trucks" (Blustein & Pincus, 2006). However, the article goes on to quote a congressional aide who helped write the original MTSA, Carl Bentzel:, "[t]hey've been saying that customs and the Coast Guard are in charge of security; yes, they're in charge, but they're not usually present" (Blustein & Pincus, 2006).

Throughout 2006, political and security actors continued debating the role of the private sector. Seaports were adapting to the new governance structures and changing rules of the security environment. Simultaneously, seaport authorities and tenants were seeing record increases in ship and container traffic. According to the World Bank, U.S. container port traffic increased nearly 44% following the slowdown attributed to 9/11, as shown in Figure 3.1 (The World Bank, 2016).

Recovering from the global slowdown following the 9/11 terror attacks, the growing interconnectedness of global supply chains, and the increasing volume of shipping, international maritime efforts were focused on shipping container security while at the same time security and economic logics were being drawn closer. As mentioned earlier, in June 2002, the World Customs Organization agreed unanimously to develop container security initiatives along the lines of the U.S. Container Security Initiative (CSI) model. By 2004, the U.S. and the European Union agreed to expand CSI throughout the European Union. Essentially, U.S. customs inspectors were assigned to foreign ports to employ "non-intrusive inspection (NII) and radiation technology to screen high-risk containers before they are shipped to U.S. ports" (U.S. Department of Homeland Security, U.S. Customs and Border Protection, CSI, n.d.).

Likewise, economic actors including importers and exporters, highway carriers, rail and sea carriers, licensed customs brokers, marine port authority/terminal operators, freight consolidators, ocean transportation intermediaries, non-operating common carriers, and Mexican and Canadian manufacturers signed on to the growing Customs-Trade Partnership Against Terrorism (C-TPAT) which essentially extended "the U.S. zone security to the point of origin… establishing clear supply chain security criteria for

members to meet, and in return, [receive] incentives and benefits such as expedited [customs] processing" (U.S. Department of Homeland Security, U.S. Customs and Border Protection, C-TPAT, n.d.).

These aforementioned programs, coupled with the ongoing port security grants, were all pushing the boundaries of the security and economic logics into closer proximity. By late 2005, the primary driving economic logics in seaports appeared to be gaining economic advantage by accommodating security actors since less bureaucratic hurdles meant faster moving goods through customs.

All of these programs were underway by the time the convergence of politicization effects from DPW, Hurricane Katrina and CNOOC giving rise to the political logic. As this triple convergence of political logics began to take hold of the public imagination, DPW became the primary focus.

Even shippers began to voice concern that increased security scrutiny of DPW ports might cause the shippers to change their port destinations (DP World, 2006). To allay concerns, the White House issued a fact sheet on February 21, 2006, clearly stating, "[t]he Department of Homeland Security (DHS) is always in charge of the nation's port security, not the private company that operates facilities within the ports. Nothing will change with this transaction. DHS, along with the U.S. Coast Guard, U.S. Customs and Border Protection, and other Federal agencies, sets the standards for port security and ensures that all port facility owners and operators comply with these standards" (The White House, Office of the Press Secretary, 2006).

In a letter to members of the Waterfront Coalition (consisting of business interests representing shippers, transportation providers, and others in the transportation supply chain) dated February 23, 2006, Ezra Finkin warned, "House International Trade Sub-Committee Chairman Clay Shaw (R-FL) intends to introduce legislation blocking the sale of any U.S. terminal operations to foreign owned companies. The vast majority of container terminal operators are subsidiaries of foreign-owned ocean carriers. In fact, the overwhelming majority of ocean carriers involved in Atlantic and Pacific trade lanes are foreign-owned companies" (Finkin, 2006). The letter went on to predict issuance of the TWIC by June 2006, which could also be affected by proposed legislation requiring all facility security officers to be U.S. citizens (Finkin, 2006).

The economic actors continued to adapt to changing rules and governance proposals well into 2006. A March 2006 policy paper from the Nuclear Threat Initiative noted "during the past decade the international maritime industry has become both increasingly globalized and concentrated, as major port operators in maritime nations have expanded their business operations by acquiring assets in a number of overseas ports. As an example of this trend, about thirty percent of port operations in the United States are performed by foreign-based firms, including eighty percent of the container terminals at the Port of Los Angeles… The consolidation of the maritime industry has also had positive effects from a security standpoint. Large port operators have both the economic incentive and the cash necessary to invest in novel security systems" (DP World, 2006).

By mid-2006, the DPW deal was off the table but the TWIC had been reinvigorated and was expected to start producing results. With the sudden interest in

seaport security, both public policy officials and security agencies were in need of demonstrable successes from their various post-9/11 institutional experiments.

3.3.3 Institutional Experiments: Initial Signs of Implementation Variance

The 9/11 Commission Report concluded that "despite Congressional deadlines, the TSA has developed neither an integrated strategic plan for the transportation sector nor specific plans for the various modes – air, sea and ground" (National Commission, 2004). The Report noted that "over 90 percent of the nation's $5.3 billion annual in the TSA goes to aviation – to fight the last war" (National Commission, 2004).

By January 2005, the TWIC was seemingly forgotten by most but not by the TSA. In late 2004 TSA had awarded a $12M USD contract to test key components of the TWIC program. Soon thereafter, however, the testing was deemed fatally flawed by the GAO. Final testing costs rose to $27M USD and "allegations of improper testing, questionable results and a contract which allowed the testing company to essentially evaluate the quality of its own deliverables created 'at least the appearance of a potential conflict of interest'" (Government Accountability Office, 2006). None of this contributed to building trust and support for TWIC from the private sector.

In June 2005, TSA's inherently flawed TWIC-pilot program was completed. However, a follow-on GAO report criticized the 2005 testing program and shed light on many of the concerns from the private sector. The GAO reported that even though there were major flaws in the proposed TWIC program, "TSA plans no additional testing of the TWIC program. Rapidly moving forward with implementation of the TWIC program without developing and testing solutions to identified problems to ensure that they work

effectively could lead to further problems, increased costs, and program delays without achieving the program's intended goals" (Government Accountability Office, 2006). Falling short of TSA's goal of issuing 75,000 port workers at 28 facilities, the testing program only issued 1,700 TWIC cards at 19 facilities. Private sector stakeholders had already voiced concerns "about the cost of implementing and operating biometric card readers, linking the readers to their local access control system, and connecting to TSA's national TWIC database" (Government Accountability Office, 2006).

Nationalization of seaport identification cards was soundly embedded in the security logics. One problem arose that the entire governance structure surrounding the cards was not also nationalized. The reality was that the TWIC program required that the private sector assume most of the burden of implementing and maintaining the program as well as potential disruptions to the labor force, both from overly strict requirements on who would be allowed to carry a TWIC and false positives in the screening process, which might unduly prevent employees from being able to carry out their day-to-day assigned tasks requiring entry into the seaport. Also, statements released from the public sector in light of the DPW crisis claimed public primacy over the security functions at seaports. However, these claims were not consistent with both the financial and operational burden being imposed on the private sector. Thus, while nationalization of the identification was part of the security strategy, there were insufficient changes in governance and decision-making authority to ensure a coordinated program.

The 2006 GAO report captures much of the growing frustration over TWIC implementation from the private sector's economic logic. Unverifiable estimates from the TSA and Coast Guard estimated each maritime facility would spend $90,000 USD to

upgrade or install access control systems. Private sector estimates far exceeded the $90,000. The GAO reported one port facility with "37 individual terminals, several of which could require 20 or more card readers for entry and exit lanes at one terminal alone. Port officials estimated that it could cost up to $300,000 per terminal to install the necessary TWIC card readers" (Government Accountability Office, 2006). This $11.1 million estimate did not include maintenance and upkeep of the system and additional costs for private sector employees to manage the new entry/exit procedures.

Port officials had also begun expressing concern about increasing delays in port terminal operations resulting from normal TWIC access let alone any emerging issues that might emerge from card reader mistakes or down time. These port operators warned that "delaying cargo entering and exiting a port could result in thousands of dollars lost by port terminal operators in the short term and millions in the long term" (Government Accountability Office, 2006).

In response to criticism from both the public and private sector, in August 2006 the Department of Homeland Security announced that the TWIC program would be implemented in two phases: "one for enrolling workers and issuing cards and the second for implementing TWIC access control technologies, such as biometric card readers" (Government Accountability Office, 2006). According to the GAO, the Department of Homeland Security made this decision "following numerous maritime industry comments about whether the access control technologies necessary to operate the TWIC program will work effectively" (Government Accountability Office, 2006). Figure 3.2, taken from the June 1, 2006, public meeting held jointly by the TSA and Coast Guard in Tampa,

Florida, displays the TWIC process model as envisioned 4 years after the original MTSA mandate.

Several new maritime security focused actors emerged during this time period including the Maritime Security Working Group and the Maritime Security Policy Coordination Committee, which resulted in the 2005 National Strategy for Maritime Security / National Maritime Domain Awareness Plan. Dedicating only 102 words specifically to the private sector, the National Strategy for Maritime Security explained that "[i]nitiatives conducted with the support of the private sector are also necessary to ensure full information dominance in the maritime domain" (U.S. Department of Homeland Security, National Plan, 2005). The National Strategy for Maritime Security goes on to reinforce that the public sector "must engage private sector organizations to include: Harbor Safety Committees, shipping companies, associations and consortia within the Global Maritime Community of Interest (GMCOI), including the National Maritime Security Advisory Committee (NMSAC) and other private sector advisory committees" (U.S. Department of Homeland Security, National Plan, 2005). This Strategy lent credence to the AMSCs, which were already hard at work.

By 2006, the AMSCs were "provid[ing] a structure that has improved information sharing among port security stakeholders… The types of information shared included assessments of vulnerabilities at port locations and strategies the Coast Guard intends to use in protecting key infrastructure" (Information Sharing Efforts are Improving, 2006).

By 2006, we begin to see divergence both in structuration and results of the two institutional experiments this dissertation is investigating. That is, as the emerging DPW

crisis was bringing attention to TSA and Coast Guard efforts to enhance port security in the wake of 9/11, the Coast Guard testified before Congress about its initial uncertainty regarding approving the DPW transaction. Clarifying the role of seaport facility operators in light of the DPW controversy, Coast Guard Rear Admiral Thomas Gilmour reaffirmed the role of the private sector and the successful implementation of the facility security plan process. Gilmour testified reaffirming what Secretary Jackson had said but also we see one of the first official accounts of the institutional experiments with seaport security plans, "I should first clarify what facility operators do. They do not run ports, and they do not provide security for the entire port system. Security for the port is the responsibility of the government and the local port authority, which is usually a government agency. However, the facility operators are responsible for ensuring the security operations within their facility are in compliance with Maritime Transportation Security regulations and executing the approved security plans for their individual facilities" (Gilmour, 2006). He later clarified, "Each operator must file a security plan for their facility with the Coast Guard, detailing how they plan to comply with all of the security measures that the Coast Guard requires. The Coast Guard then inspects the facility and checks the execution of the plan, requiring more effective measures if they are deemed necessary. There are over 3,000 marine cargo facilities in the United States and each has an approved and inspected security plan." (Gilmour, 2006).

During the same testimony, Gilmour explained what the role of DPW would be and why it was not that strategic in terms of security. He went on to describe that facility operators generally build piers and add cranes for loading and unloading cargo. The

DPW deal only involved six ports and, of the 800 regulated port facilities at those ports, DPW would operate only 24 of them (Gilmour, 2006).

Interestingly, we begin to see differences between the implementation of the TWIC program and the Maritime Security Planning processes described above by Admiral Gilmour. Although the MTSA was nearly four years old by the time Rear Admiral Gilmour testified, TSA's TWIC had made little real progress and virtually none with respect to improving security conditions, whereas the Coast Guard's partnership with the private sector with respect to the security planning functions was already demonstrating a merging of the security and economic logics.

3.4 Act III: 2007 to 2012: Economic Logics Gain Salience Yet Again

"The further away we get from 9/11, the further we slip into what we were on September 10, 2001, not what we were on September 12th, 2001. We slip back into that state of complacency, and just thinking that's not going to happen to us." - Mark R. DuPont, President/CEO, Merrick Maritime Security, Inc., Director, NASBLA Boat Operations and Training Program (Personal Communication, February 22, 2016).

The nation started to see a shift in seaport security mindsets by late 2005. Economic logics had caught up with security and was starting to make itself felt when the national dialogue was temporarily sidetracked by the DPW fiasco and the brief rise in political/state logics during a congressional mid-term election. However, by 2007, the DPW issue was well behind and the economic logics began gaining preeminence in seaport security conversations once again.

During this third time period, 2007 to 2012, we begin to see the outcomes of various institutional experiments set in motion in the wake of 9/11. We see the fruits of the labors

of new, post-9/11 security actors and the variance associated with the degrees of effectiveness and sustainability. Particularly, the TWIC and the AMSP were two such institutional experiments. Both began around the same time with generally the same stakeholders in most cases. Yet, the various logics and the degree to which those logics integrated ensured that new rules and new governance structures were brought into being. The degree to which these two programs were received and implemented draw stark contrast. One cost tens of millions of dollars with little to show while the other had a minimal financial cost but created a collaborative environment that will prove invaluable in the years ahead. The long term effects of a punctuated international terror attack on the business environment are both simple and complex, mundane and profound at the same time, it seems.

3.4.1 Transportation Worker Identification Credential (TWIC): Institutional Experiment Falls Short of Expectations

As an institutional experiment, the TWIC program was set in motion with passage of the Aviation Transportation and Security Act of 2001 and the Marine Transportation Security Act of 2002 at a time when security logics was in the forefront. Over the ensuing years, the TWIC had begun to fade until the political logics associated with the DPW crisis brought it back to the front burner and suddenly it became a priority for the public sector driven by both political and security logics. However, as the TWIC progressed to implementation and beyond, the economic logics began to resurface as TWIC users were faced with the reality of a nationalized identification card. To recap the TWIC thus far, Figure 3.3 presents the key actions taken by Department of Homeland Security agencies while nationalizing the seaport identification card.

Originally, the TWIC had been assigned to two agencies: TSA and the Coast Guard. As a new security actor after 9/11, the TSA assumed the lead role in the initial roll-out of the TWIC. However, the entire process had amounted to nationalization of the security credential without nationalization of the full governance structure behind administering the day-to-day program in the field. In TSA terminology, the initial approach to TWIC, as shown in Figure 3.4 (a TSA PowerPoint slide from a briefing in 2003), was entitled "Federally Led Public/Private Partnership"; however, the implementation was far different from what is shown in Figure 3.4. The more appropriate terminology would have been nationalization of the access identification credential. By 2007, after a series of missed opportunities and confusing policy shifts, much of the early goodwill on display from the maritime community had diminished and trust had eroded between the private and public sectors with respect to the TWIC.

As far as trust is concerned, a Director of Security for a major maritime operation spoke with me regarding personal experience working with TSA and a vendor during the TWIC reader testing:

> …and they would see how many failures there were; all the issues that ran into it; And the data it presented… we ran it for 9 months and during the 9 months it was clear that it was an issue with a lot of employees transiting… into and out of restrictive areas… [But the TWIC reader program failed] so the report came out, the draft report, and we sat with the vendor and TSA and we basically said there was a 40% failure rate. And we all agreed it was a big failure rate and all this. But when the final report came out, [TSA and the vendor] attributed the significant failure rate to operator error… it was fully monitored by college graduates from maritime academies… smart people who knew how to manage the process… but [the technology] failed. It continued to fail… but they chose to say operator error at 40%... we were all kind of bitter because they changed the final report on us (Interview 32, 2016).

In January 2007, the TSA and Coast Guard finally issued the final rule implementing Phase One of the TWIC. The public was notified that the enrollment process would begin no sooner than March 2007 in a limited number of ports before eventual expansion throughout the country. Nearly 5.5 years after 9/11, however, and the forthcoming TWIC had no substantive improvements than the type of "flash pass" identification cards issued by various ports prior to 9/11. "While the TWIC will be a smart card, with encrypted biometric data, the requirement for installation and use of a card reader will be delayed for a future rulemaking (phase two). In the meantime, the TWIC card will function as a photographic identification" (Transportation, 2007).

In January 2007, the Sailors Union of the Pacific wrote in a newsletter describing the labor union's efforts to block the TWIC: "Forcing a cost [port security] that should properly be the government's onto the maritime workforce is one thing, but to do it for a card that may never be used as intended is quite another. We urge you [DHS] to be fair to the nation's maritime workers and direct TSA to stop the entire program until it can be implemented as Congress intended" (Maritime Labor Testifies, 2007).

Testifying about TWIC before Congress, American Waterways Operators President & CEO Tom Allegretti "conveyed the towing industry's concerns that the TWIC would exacerbate the already severe personnel shortage" and suggested that an amendment be approved allowing a worker to work for 90 days before requiring a TWIC, presumably to avoid hiring delays (AWO, 2007).

At the same hearing, Mike Rodriguez, of the International Organization of Masters, Mates & Pilots, testified on behalf of a joint Labor Union statement. Rodriguez

covered a host of TWIC topics including competitiveness. Rodriguez explained that foreign crews (not subject to the TWIC) were responsible for 95% of the cargo entering and leaving U.S. ports. "Foreign crews are not covered by the TWIC program…. are not subject to U.S. government imposed background checks. Consequently, the overwhelming majority of maritime personnel responsible for the carriage of hazardous and other cargoes in and out of our country will not have to obtain a TWIC or obtain an access control credential issued by American states, ports and facilities – only American mariners will be subjected to these numerous and onerous requirements" (Maritime Labor Testifies, 2007).

In 2012, the Transportation Trades Department of the AFL-CIO[6] also testified about the financial implications of the TWIC. Larry Willis said his unions were "vehemently opposed" to the concept that individual workers had to bear the cost of the TWIC: "The security threat assessments and the background checks mandated in this proposal are considered necessary to enhance the security of our nation's ports and are

[6] List of affiliated unions: Air Line Pilots Association (ALFA); Amalgamated Transit Union (ATU); American Federation of State, County and Municipal Employees (AFSCME); American Federation of Teachers (AFT); Association of Flight Attendants-CWA (AFA-CWA); American Train Dispatchers Association (ATDA); Brotherhood of Railroad Signalmen (BRS); Communications Workers of America (CWA); International Association of Fire Fighters (lAFF); International Association of Machinists and Aerospace Workers (lAM); International Brotherhood of Boilermakers, Iron Ship Builders, Blacksmiths, Forgers and Helpers (IBB); International Brotherhood of Electrical Workers (IBEW); International Longshoremen's Association (ILA); International Longshore and Warehouse Union (ILWU); International Organization of Masters, Mates & Pilots, ILA (MM&P); International Union of Operating Engineers (lUOE); Laborers' International Union of North America (LIUNA); Marine Engineers' Beneficial Association (MEBA); National Air Traffic Controllers Association (NATCA); National Association of Letter Carriers (NALC); National Conference of Firemen and Oilers, SEIU (NCFO, SEIU); National Federation of Public and Private Employees (NFOPAPE); Office and Professional Employees International Union (OPEIU); Professional Aviation Safety Specialists (PASS); Sailors' Union of the Pacific (SUP); Sheet Metal Workers International Union (SMWIA); Transportation Communications Union/lAM (TCU) Transport Workers Union of America (TWU); United Mine Workers of America (UMWA) ; United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW); and United Transportation Union (UTU). (Source: Willis, 2007)

part of the overall effort to fight terrorist elements. Given the reality of this national priority, the government, and not the individual workers, must absorb the costs of this program" (Willis, 2007). Again, economic logics pushing back against the security logics that had driven the TWIC for years.

For years, the GAO had testified before Congress about the progress and challenges associated with the TWIC. Some of these challenges directly reflect the effect of the security logics and nationalization of the identification without the subsequent changes in governance structures. Thus, whereas TSA and the Coast Guard "owned" the TWIC, much confusion remained in the private sector regarding TWIC reader stations, capabilities of those stations, how the biometric data on the cards would be updated and compared to the national database in real time, who would operate the stations, who would pay for the TWIC inspection processes and even what type of card readers were out even authorized for use. Needless to say, due to the governance structure changes, we see large disconnects by 2007 and 2008 in terms of private sector "ownership" of the nationalized process.

Nearly five years after first being introduced, the TSA and Coast Guard "issued the first rule in federal regulation to govern the TWIC program, setting the requirements for enrolling maritime workers in the TWIC program and issuing TWICs to these workers" in January 2007 (Government Accountability Office, 2008). However, frustration was growing. A former security official explained the frustration with TSA during some of the early phases of the TWIC roll-out and why that frustration had accumulated over the years from industry. The official explained during an interview that in the beginning TSA's main focus was airports and aviation. With respect to the

Port of Charleston, the TSA office was set up at the airport, not the seaport. Then, once TSA contracted out the whole TWIC program, it was obvious that they just were not "plugged" in" (Interview 24, 2016). The January 2007 TWIC rule outlined many of the impacts expected to be felt by the private sector as seen in Figure 3.5.

Early in 2008, the American Trucking Association wrote a letter to TSA about the number of identification cards required by its members: "Unfortunately, the TWIC program/concept has not lived up to its promise. Today, truck drivers must obtain a TWIC to access secure areas of port facilities, an HME [hazardous materials endorsement] to transport hazardous materials, a FAST [Free and Secure Trade] card to cross the border, a SIDA [Secure Identification Display Area] check to access airport facilities, and individual credentials to access certain chemical facilities and railroad transfer stations. The original objective of TWIC has not been achieved" (Rojas, 2008).

The TSA had been enrolling TWIC carriers and "as of September 12, 2008, 497,928 enrollees, or 41 percent of the anticipated 1.2 million TWIC users, have enrolled in the TWIC program. Further, 318,738 TWICs have been activated and issued" (Government Accountability Office, 2008).

Ironically, in an effort to simplify the TWIC implementation process, this first phase did not include information about how owners and operators of maritime transportation facilities and vessels would implement the card reader program to take full advantage of the advanced biometric features that were originally part of the reason for nationalizing the card in the first place. The Director of Security for a major seaport authority provided a summation of the card:

> A grandiose idea that had its place in the - some would say - overreaction to 9/11. Idea at the time is that it was going to cover maritime, aviation, road, bus, rail… workers as a single federal credential for all transportation workers. Certainly, in the aviation world there already was a credential that already had at least a federal background check but they were locally produced. In our conversation I'll keep coming back to the aviation credential because there are some really good things in that model that work that we don't have in the TWIC model. But because TWIC has been so long in coming out as what it was originally envisioned to be even from a technology perspective not necessarily from the scope of all transportation workers, there is minimal value I think in what it provides. TWIC as a credential issued to workers after successful completion of a federal background check and to be used as a smart card so that it is a who you are, what you know, and what you have - so a pin, a biometric and a physical credential - those *who you are* and *what you know* have never been put into place as a national standard or a national requirement, nor has the physical verification of the card - the validity of the card been put into place. It's just a flash pass. It's just a hold it up to the guard and you are good to go (Interview 23, 2016).

As a result, taxpayers had contributed $103.4 million USD in appropriated funds for a government-issued identification card that was no more effective than any pre-existing cards had been (Government Accountability Office, 2009).

In July 2008, the National Maritime Security Advisory Committee's (NMSAC) TWIC Working Group issued a scathing assessment and recommendations regarding the TWIC program. We see the economic logics gaining ascendency as the TWIC program moved into actual implementation and eventual maintenance phases. Though lengthy, the list of NMSAC-generated TWIC problems provides a compelling picture of the outstanding issues after 6 years and $100+ million USD spent. The NMSAC warned both the TSA and Coast Guard that "[u]nresolved problems in each of the areas addressed below help to foster the sentiment among stakeholders that the TWIC program is broken. Coast Guard and TSA must address the issues identified in each of these areas if they hope to generate higher rates of enrollment, sustain stakeholder cooperation and meet

compliance dates" (National Maritime Security Advisory Committee, 2008). Appendix C contains a partial list of these identified problems.

Finally, the April 2008 NMSAC comments reported that "[d]espite the fact that the initial TWIC roll-out is already halfway complete in terms of estimated timeframe, only approximately 219,000 of the estimated 1.5 million potential TWIC holders, or just over 14%, have received their cards. Clearly, there are a number of issues that need to be addressed even this far into the process" (National Maritime Security Advisory Committee, 2008).

As previously mentioned, TSA was required to speed up its implementation schedule of TWIC roll-out. The phased-in approach was designed to roll out the program by geographic region using Captain of the Port (COTP) zones. Thus, the roll-out schedule eventually took place as shown in Table 3.1 (part 1) and a map showing the zones (part 2).

However, the roll-out was not without complications. In October 2008, the TSA experienced a power outage at TWIC processing facilities that was not fully resolved until late November. As a result of this outage, TSA announced that equipment used to reset personal identification numbers for thousands of holders of the TWIC was permanently damaged; consequently, those who could not remember their TWIC pin numbers would have to relinquish their current TWIC and be reissued a replacement (Lipowicz, 2009). According to the GAO, the cost of replacing these cards was more than $26 million USD (Government Accountability Office, 2009).

Ten years after 9/11, the TWIC program continued to under-impress. Returning to Figure 3.3, it is important to note that while the figure states all nationwide ports are in compliance with TWIC requirements as of 2009, some key information is left out (*e.g.*, no biometric capabilities). For instance, a scathing 2011 GAO report to Congress enumerated a list of mistakes by the Department of Homeland Security that called into question the integrity of the card itself and the system in place for screening and distribution. According to the GAO, the Department of Homeland Security had not:

- assessed the TWIC program's effectiveness at enhancing security or reducing risk for MTSA-regulated facilities and vessels;
- demonstrated that TWIC, as currently implemented and planned, is more effective than prior approaches used to limit access to ports and facilities, such as using facility specific identity credentials with business cases; and
- conducted a risk-informed cost-benefit analysis that considered existing security risks, and it has not yet completed a regulatory analysis for the upcoming rule on using TWIC with card readers (Government Accountability Office, Pub. No. 11-657, 2011).

The GAO report also noted that "[c] onducting an effectiveness assessment that further identifies and assesses TWIC program security risks and benefits could better position the Department of Homeland Security and policymakers to determine the impact of TWIC on enhancing maritime security" (Government Accountability Office, Pub. No. 11-657, 2011). By June 2011, nearly 1.77 million TWIC cards had been activated from the 1.9 million enrollment applications received (U.S. Department of Homeland Security,

Transportation Security Administration, 2011). These numbers continued to climb and by May 17, 2012:

- 2,176,274 individuals are enrolled in the TWIC program;
- 2,023,780 TWICs have been activated;
- 105,298 initial disqualification letters have been issued;
- 50,184 appeals requested;
- 48,957 appeals granted;
- 11,826 waivers requested;
- 10,238 waivers granted;
- 2,086 final disqualification letters issued;

Of the 2.1 million individuals enrolled in the TWIC program:

- 805,776 are truck drivers;
- 384,720 are rail workers;
- 316,417 are merchant mariners;
- 267,543 are port workers including terminal employees, longshoremen and drayage truckers.

(Review of the Delays and Problems, 112th Cong. 2, 2012).

In 2012, the International Longshore and Warehouse Union (ILWU) called for the entire TWIC program to be terminated. ILWU legislative director, Lindsey McLaughlin said, "TWIC offers very little benefits and… it would be wiser to spend this money on other port security initiatives… We strongly encourage Congress to stop throwing money at ineffective programs. A wiser approach to port security would be to invest these federal dollars into Customs, the Coast Guard and other federal agencies to implement container security and intelligence programs rather than spending billions more on TWIC" (ILWU, 2012).

By June 2012, the TWIC program was under intense scrutiny. Multiple congressional hearings had been held over the spring and multiple stakeholders were increasingly vocal that the security benefits of the card did not justify the cost in time and money. Opening one hearing, Congressman John Mica (R-FL) lamented, "and now we

are going to face again the cost of deploying cards that have become almost a joke with the transportation community" (Review of the Delays and Problems, 112th Cong. 2, 2012). Even though the TSA would not participate in the hearing, the Department of Homeland Security was represented by an Acting Deputy Assistant Secretary (DAS). Extolling the many security benefits of the TWIC, the DAS explained that TWIC was a "public/private-sector relationship" and while the Department of Homeland Security does the background check, the private sector (*e.g.*, facilities and vessels) use the TWIC while enforcing their own security. "DHS also partners with the private sector by participating in regular meetings with a TWIC Stakeholder Communication Committee, speaking at conferences, and visiting MTSA regulated sites to see the TWIC program in operation" (Review of the Delays and Problems, 112th Cong. 2, 2012).

U.S. Coast Guard Admiral Joe Servidio also testified of the primacy of the private sector when it came to TWIC. He noted that simply possessing a TWIC was not justification for access all areas of facilities and vessels. Rather, the TWIC was a tool to be used by the private sector security officers to "inform the security officer's decision to grant unescorted access to an individual" (Review of the Delays and Problems, 112th Cong. 2, 2012). Beyond that, a maritime industry security director told me in an interview that "[j]ust because you have a TWIC doesn't mean you can get into our restricted areas. You have to have a second piece of identification [our photo ID] to either bring your car in or yourself" (Interview 32, 2016)

However, a terminal operator explained that reality might be a bit different:

> Anytime there is a security incident we call it a TSI - a transportation security incident – within the confines of our security plan under 33 C.F.R. 105. I'll give you a perfect example. Most of the trucks coming into our facility are over the road sleeper trucks. 9 times out of 10 my guys will stop them. We are required to vet but we can't search and we have no jurisdiction or expectation to go inside the vehicle because we are not law enforcement. So what we'll ask the driver, 'Do you have anyone in the truck?' and he'll say no we don't. So they'll go through and pick up their container. Meanwhile the guys in the back sleeping if he's his friend, his brother, his kids whatever the case may be. Eventually either my security patrol will pick up on two people in the truck and will stop them in the confines of the yard and say show me your TWIC card and he won't have one. Or Customs and Border Protection will catch them on the out-gate check at the radiation portal. So now we have this guy who got in in the restricted area with no TWIC. The Coast Guard is supposed to physically come to the facility to retrieve the individual's TWIC… so he basically doesn't have a TWIC anymore. But they've never done that in the [x] years I have been here. So what will happen is, Customs and Border Protection has been deputized to basically act like Coast Guard officers and basically take that TWIC card from the individual who acted illegally, but I've never seen that either… so I'll send the report in and I'll get no less than 15 phone calls from every law enforcement agency in the country... from the state police, port authority police, homeland security police – all asking the same question because they don't talk to each other – how'd that guy get inside your terminal? Eventually I'll get a call from the command center of the Coast Guard saying what are you going to do about it? I tell him, 'Nothing. I'm not doing anything about it.' I'll be honest with you, why even report it anymore? I mean, what's the point? ... And this is collectively, this isn't unique to my facility. This is just how things operate… I don't know who you have been talking to that said TWIC is this great thing. The whole program is flawed and doomed to fail... It sucks. (Interview 15, 2016).

The TWIC provides a means by which a vessel or facility security officer can determine that an individual has been vetted to an established and accepted standard using a single, uniform, tamper-resistant credential that security personnel has been trained to examine. In July 2012, the American Chemistry Council (ACC) (representing the 800,000 Americans involved in the chemical industry) wrote in favor of the Terrorist Screening Database checks done to TWIC applicants. The ACC affirmed that these checks were of "significant value to the industry although it is an inherently

governmental function and can only be performed by the U.S. Department of Homeland Security" (Dooley, 2012).

Joe Lawless, Director of Maritime Security at the Massachusetts Port Authority (Massport) and Chairman of the Security Committee at the American Association of Port Authorities stated that "TWIC mandates have changed the way port facilities are run. In addition to the cost of the card, port facilities must now ensure that all gate and entrance points have a way to check TWICs. Massport staffs all of its access points into our facilities with security personnel to verify that the entrants have a TWIC" (Lawless, 2012). However, Lawless goes on to point out that the much-vaunted biometric aspects of the credential are not in use and that delays with the proposed card readers mean that the "TWIC is currently being used as a flash pass" (Lawless, 2012).

Speaking to representatives from Labor Unions and Seaport Authorities, Representative Mica reported that Congress had "heard the frustration of both labor and also our ports, the association that runs the ports throughout—and represents the ports throughout the Nation. What we have in place is not acceptable. The delays are just beyond comprehension. The inability to put this program together is startling. And then the cost to the taxpayers in financing this entire fiasco is just totally unacceptable— a $3.2 billion program which is rife with problems and does not secure our ports" (Review of the Delays and Problems, 112th Cong. 2, 2012).

By 2012 the security logics that had driven development of a biometric identification credential for all modes of transportation had not resulted in a viable program. The economic logics and $3.2 billion in taxpayer money spent made the future

of the project questionable at best. Representative John Mica had harsh words for the TWIC program when he stated that the TWIC "was no better than a library card" (Review of the Delays and Problems, 112th Cong. 2, 2012).

As the rollout of the TWIC continued, pushback came from multiple sectors. Labor had been opposed to the strict past criminal history checks keeping workers from being approved for the identification card. Labor unions were concerned that TWIC applicants were being misidentified, unfairly investigated and that past transgressions with little or nothing to do with terrorism were preventing them from being authorized a TWIC. "Around 75% of those denied a TWIC (close to 50,000 people) appealed and 99% of appeals have been granted. The appeal process takes around 6 months and the appellant cannot work at a port in the interim" (ILWU, 2012).

At the aforementioned 2012 congressional hearing on the TWIC, where the TSA did not testify despite an invitation, Admiral Servidio drew a clear distinction between agency responsibilities: "To clarify agency roles regarding the TWIC program, TSA is responsible—the Transportation Security Administration—for TWIC enrollment, security threat assessment, adjudication, card production, technology, TWIC issuance, conduct of the TWIC appeals and waiver processes, and management of government support systems. The Coast Guard is responsible for establishing and enforcing access control requirements at MTSA-regulated vessels and facilities, which include the requirements for TWICs at approximately 2,700 regulated facilities, 12,000 regulated vessels, and 50 regulated Outer Continental Shelf facilities" (Review of the Delays and Problems, 112th Cong. 2, 2012).

Thus, eleven years after 9/11, the security agencies guided by the public sector security logics were under increasing criticism as the logics paradigm shifted and economic logics gained ascendency. In the final weeks of 2012, the Department of Defense announced that the TWIC program mandated 10 years earlier and managed by the Department of Homeland Security "did not meet Department of Defense security standards. Serious questions need to be asked about why this multimillion-dollar program has failed" (Krepp, 2012).

3.4.1.1 Labor Market Implications

"Then you get to that point and you have to figure out how we break these policy barriers down. Then the TWIC program doesn't do itself any favors, you have a guy that ends up on a [Navy Ship] that gains access to the facility using a TWIC card and ends up shooting a few people at a Navy installation outside of Norfolk." (Interview 16, 2016).

One of the issues security logic driven programs must consider is that implementing multi-dimensional programs in complex environments like seaports may have cascading effects and unintended consequences beyond the original intent. As stated earlier, one of the primary implications for TWIC was on the labor force. As the TWIC program languished over ten years, it had an impact on the livelihood of people working in the seaport industry. A security official at a major seaport explained that the real disruption from the TWIC program was more than someone simply taking time off work to get their fingerprints, photo, etc… but in some cases it has taken months for employees to get new or replacement TWICs (Interview 23, 2016). There are many documented cases of employees unable to gain access due to delays or disruptions receiving their TWIC cards. This same official told me that they had "…one employee who has waited a year before [receiving the TWIC]" (Interview 23, 2016).

A former high ranking security official had voiced concern that the TWIC would have the effect of further limiting the pool of available labor with harmful economic consequences. His concern was that the same time TWIC was being developed, several other phenomena were occurring in the marine industry which also contributed to constricting the labor force. Simultaneously, the world was experiencing increases in port capacity, size of ships, number of containers being transported, saturation of geographic port space and more operations, thus increasing labor needs on the one hand while on the other hand, the marine industry labor pool was constricting due to a push toward smaller environmental footprints coupled with the introduction of new cyber and artificial intelligence/increased automation. As a result, the very nature of the maritime industry was experiencing tension with labor needs even as the TWIC was rolling out. This security official's concern was that the perceived labor force reduction resulting from workers who were going to be denied TWICs was going to exacerbate the overall economic situation in the maritime industry (Interview 6, 2016).

In terms of managing the public-private interface, it was unclear whether TSA fully appreciated that the increasing cost of operations (*e.g.*, every new security rule being introduced, whether regarding advanced notice of arrival, seafarers access rules, vessel reporting requirements, etc.) would add increasing pressure to the already economically volatile labor situation (Interview 6, 2016). As it turned out, so many waivers were given for seaport workers who failed their initial TWIC application that the resultant restriction in labor pool never materialized.

Nevertheless, I spoke with many representatives from multiple labor unions in the process of field research for this study and I received many stories about unexpected

hardships endured by laborers as a direct result of the TWIC. A president for an International Longshoremen's Association (ILA) Local explained their role in the seaport and how the TWIC has made it more difficult. His union provides union labor on demand. Each day by 5 p.m., shipping companies and others call and tell the ILA Local that, for example, two hundred workers are needed tomorrow the next morning. Then, possibly, two days later only thirty workers are needed. As a result, ILA Local members frequent the union hall to learn what labor orders need to be filled. The shipping companies and those needing the labor have an opportunity to cancel their orders with little to no notice; however, at times the ILA Local scrambles at the last minute to find workers. This is where the TWIC complicates things. Before TWIC, the ILA Local could phone members and invite them to bring along a son or friend for temporary work. This interviewee continued to explain that because everyone now has to be pre-certified with a TWIC, now there are times that the union cannot fill large orders, which then means the ship takes longer to load and offload: "In the past, we picked up new members all the time from the people who would occasionally come in for just the large orders. Now, TWIC has had an impact on our new membership as well." (Interview 35, 2016).

This interviewee also explained that the original list of criminal offense disqualifiers for the TWIC program did not make sense. Just because someone had a criminal background once does not make him or her a threat to the country while moving cargo around a pier. He said, "[t]he one thing I love about the waterfront is the fact that it's a place of second chance… So many success stories on the docks. People made mistakes early in life, then came out here, earned good income, married, bought a home,

success stories you can't imagine. But now, it is not always the case. Your background is going to follow you for seven years" (Interview 35, 2016).

An alleged unintended benefit for the dockworkers' unions was the TWIC's sudden impact on non-union workers. "Those unscrupulous employers using undocumented workers," alleged a union representative, were siphoning off work from unionized companies getting cheaper, non-union labor (Interview 35, 2016). He explained that when the port was considering new rules for TWIC, his union managed to get entire terminals segregated as "sensitive" areas, thereby ensuring that someone without a TWIC could not work on that terminal without being escorted by a pre-approved TWIC carrying member. This reduced non-union hiring and created hurdles for undocumented workers (Interview 35, 2016).

Another seaport expert reinforced the union position above that the TWIC rules on past criminal behavior were "rammed through" by those who did not think dockworkers should have murder or drugs in their backgrounds (Interview 25, 2016). This interviewee's opinion was that someone who had committed a violent crime is not necessarily a security threat, so non-security related offenses should not have precluded a worker from obtaining a TWIC and thus being allowed to work on the seaport (Interview 25, 2016). Nonetheless, most interviewees did relate that TSA had been effective in explaining the TWIC requirements before the roll-out.

To fully appreciate the scope of the workforce affected by the TWIC roll-out, the International Brotherhood of Teamsters (IBT) issued a fact sheet to its members. The following IBT members would be required by regulation to obtain a TWIC: "[p]ort

employees, longshoremen, mariners, truckers, and others who require unescorted access to secure areas of ports and vessels would be required to be vetted under the TWIC program. The IBT represents more than 5,500 longshoremen, clerks, truck drivers, tugboat deck hands, tug boat captains, port authority employees, guards and warehousemen who work in our nation's ports" (International Brotherhood of Teamsters, 2007).

Laura Moskowitz from the National Employment Law Project testified before the House of Representatives in 2008: "[i]t has become increasingly apparent that foreign-born applicants[7], including military dependents born on bases abroad and other U.S. citizens, are being denied in large numbers even though they are TWIC-eligible… Indeed, about two-thirds of all appeals are based on citizenship or immigration status issues" (Moskowitz, 2008). Moskowitz continued, "[l]arge numbers of foreign-born workers are finding themselves in this situation, driving up the number of appeals sent to the adjudication office and placing an unfair burden and stigma on foreign-born workers" (Moskowitz, 2008).

This last quotation highlights the single biggest impact TWIC has on with respect to security in seaports: it has effectively banned foreigners from working without an escort in areas requiring a TWIC card. This was particularly evident in several interviews I conducted including the aforementioned union representatives. Although the

[7] For clarification: TWIC eligibility is limited to U.S. citizens, lawful permanent residents, naturalized citizens or a nonimmigrant aliens, asylees, and refugees who are in lawful status (Source: U.S. Department of Homeland Security, Transportation Security Administration, n.d.).

unions had expressed concern about union members being denied TWICs due to past criminal activity, TSA's easing of the approval criteria for receiving a TWIC ensured that this became almost a non-issue for most applicants. In addition, an appeals process was created for anyone not receiving approval for their TWIC application. While exact numbers are difficult to find, most interviewees stated that they knew *no one* who had been denied a TWIC after their appeal. Concurrently, the unions had been seeing illegal migrant workers being hired to replace union members prior to issuance of the TWIC. One of the unforeseen but positive elements (at least in the eyes of the unions) is that undocumented, illegal migrants were unable to obtain a TWIC due to the U.S. citizenship requirement. This effectively resulted in one of the only tangible, unique benefits resulting after 10+ years of TWIC implementation: prevention of non-U.S. citizens from entering (without an escort) TWIC-controlled areas of port facilities. With a TSA-credentialed escort, foreign nationals are allowed to be on the premises but there are strict regulations (at least on paper) about how these escorts are conducted.

Keep in mind, however, that the "foreignness," as evidenced by the DP World debacle, was not applied equally to all foreigners in non-TWIC related security issues. After all, P&O was a British company that DP World bought out. There was no particular concern about British ownership but only when the Arabs became involved. The TWIC, on the other hand, appears to be the great equalizer as far as foreign citizenship is concerned. Aside from foreign national in various stages of visa approved residency, a foreign national cannot simply walk into a TWIC application service center and receive a TWIC.

Since the TWIC is only required for access to restricted areas, terminal operators and others have had to be "creative" in how they defined these secure areas. (Note: The following is paraphrased from an interview I conducted with a terminal operator):

> We had a waterfront facility with bulk oil storage and suddenly we were told we would need TWICs onsite. We had huge oil tanks with large containment berms that could have been breeched. After 9/11, we added private security guards but the idea of bullets moving around a high energy pipeline made us less than desirable. We considered the entire facility at first but eventually cordoned off the smallest footprint that we could to minimize the physical space where TWIC entry would be required. So, instead of the whole staff requiring TWICs, only one engineer per shift needed one. Others in the industry have been innovative in their approach to which areas would be marked as TWIC-required as well. From a compliance standpoint, the government has to understand what they want to accomplish. Simplicity is elegance" (Interview 6, paraphrased, 2016).

Still, even as the marine industry has found solutions to minimizing the number of TWICs required on staff, foreign nationals remain the one group the TWIC has barred without escort.

In June 2013, President Wykind of the Transportation Trades Department of the AFL-CIO issued a statement regarding the TWIC program entitled "Time to Reconsider Flawed TWIC Program." Wytkind said, "[a]s the Government Accountability Office (GAO) recently concluded, after 11 years since the TWIC program was first conceived, with 2.3 million cards issued and hundreds of millions of dollars spent, the security benefits of this initiative have not been demonstrated. While the GAO has suggested yet another 'assessment' to confirm what we already know – that the program is inherently flawed" (Wytkind, 2013).

Consequently, the concept of cascading effect and unintended consequences must be considered whenever a security-logic driven institutional experiment is implemented.

3.4.2 Area Maritime Security Committees / Plans: Institutional Experiments Exceed Expectations

The long term viability of the Coast Guard's approach to collaborative seaport security efforts is evident with the AMSC's successful delivery of complex threat analyses and AMSPs. The blending and eventual integration of security and economic logics resulted from new players changing the governance structure following 9/11. The Coast Guard's ability to build partnerships in this complex environment was driven home to me during an interview I conducted over the course of this dissertation with a maritime security expert. DuPont told me, "I use this example from the Apollo movie with Tom Hanks… when they realize that they have a problem, all the engineers in the room come together and they dump everything on the table… get a bunch of smart engineers and ask what can be done… [the] USCG does the same thing" (M. DuPont, personal communication, February 22, 2016).

The intent behind implementation of AMSCs was to provide a structured environment for port stakeholders to collaborate on a routine basis and to foster dialogue amongst stakeholders and even competitors with a holistic approach to port security. The AMSC was then to conduct risk assessments and eventually aid in the creation of the AMSPs. With the Coast Guard's Captain of the Port (COTP) designated as the Federal Maritime Security Coordinator (FMSC), it is easy to envision a different scenario wherein the Coast Guard conducted the port assessments on behalf of the marine industry and then issued a port security plan with little or no input from the other stakeholders. However, the entire Coast Guard, though smaller than the New York City Police

Department, was often viewed as an honest broker and a maritime partner and assumed the same role in this process.

As one maritime professional explained, "those partnerships were really key… 9/11 really cemented in people's minds that key stakeholders in the maritime community knew it was worth their time to engage in these committees even though in dollar and cents terms it costs a lot of money to have people really engaged in these committees… they saw the value of these partnerships. The Coast Guard is really good at playing a leadership role in bringing people together" (Interview 5, 2016).

Another port stakeholder explained the structure of the AMSC in their port:

> [there is] a Board of Directors - 3 [representatives] from the public sector and 3 from the private sector and of course the Captain of the Port serves as Chairman of the Board. About 3 Captain of the Ports ago, Captain [unintelligible] made it a point to say that everyone knows the Captain of the Port is in charge. He is the designated Federal Maritime Security Coordinator, etc. etc. so he sort of set the tone and said he wanted the Chairman and the Vice Chairman of the AMSC to come from industry because they are going to be here, I'll leave in 3 years and the next Captain of the Port will leave 3 years after me. He wanted corporate continuity and didn't want upheaval (Interview 9, 2016).

The previous quotation provides a real sense of the personal commitment to collaboration that was a hallmark of the AMSCs and likely led to their success drawing upon existing structures for legitimacy and experience. The first tasks for these committees revolved around a "family of plans." This family of plans[8] included vessel security plans, facility security plans, and port security plans in addition to the port security risk assessments. The AMSCs were focused on first conducting the port security

[8] The Facility Security Plans were explained in the Navigation and Vessel Inspection Circular (NVIC)11-02, which provided guidance for development of uniform security programs at marine facilities. Vessel Security Plans were described in NVIC 10-02 and the Port Security Plans were initially described in NVIC 09-02, which provided an overview of security to be implemented at the port level (Tuebner, 2003).

risk assessments and then using this information to conduct the port security plans, which became known as the AMSPs.

Concurrently, the International Code for the Security of Ships and of Port Facilities (ISPS) Code amended an international agreement, SOLAS Chapter XI, to mandate that port security plans were to be completed by July 2004. The ISPS Code also required port facilities that received ships on international voyages to conduct security assessments and to develop security plans. The Coast Guard amended the date requiring all plans to be completed by December 2003 and approved no later than July 2004 (Tuebner, 2002).

Initial assessment guidance assigned leadership of the port security assessment process to the COTP who would work with a Port Security Committee to conduct the assessment. The process would begin with selecting targets leading to a decision based on consideration of the following trade-offs associated with: targets/threat, criticality, scenarios, consequences, vulnerabilities, document/mitigate/consider, mitigation strategies and trade-offs. Committees were told to consider the following as well:

Security vs. Access
- Security measures may restrict use of waterways
- Security measures may restrict access to information

Security vs. Commerce
- Security measures direct and indirect costs

Security vs. Environment
- Security initiatives may take resources away from pollution prevention & response
- Security measures may require that more land & water be available for commercial use – staging & screening areas, buffer zones, natural barriers

Security vs. Safety
- Crew fatigue due to additional duties
- Access controls limit resources on hand to respond to "near misses" (tugs, line handlers, etc.) (Tuebner, 2003).

It is not so much these technical details are important as it is to understand the complexity of the task at hand and what was expected of these new governance structures. Consisting of public and private representatives, the AMSPs and the security assessments were completed in a timely fashion with actual institutional outcomes. Likewise, these AMSPs (primarily seen as a communications and coordination document) resulted in actual changes in the rules of seaport security that included:

- Details of operational and physical measures that must be in place at all Maritime Security (MARSEC) Levels;
- Expected timeframes for responding to security threats and changes of MARSEC Levels;
- Communications procedures;
- Measures to ensure the security of vessels, facilities, and operations that are not covered by the security requirements in other parts of this subchapter;
- Measures to ensure the security of the information in the AMS Plan;
- Periodic review, audit, and updating procedures;
- Procedures for reporting security incidents; and
- The jurisdiction of Federal, State, Indian Tribal, and local government entities over area security related matters. (Maritime Security, 2003).

There are other examples as well but the simple fact remains that these institutional experiments were very successful. They were so successful that the AMSCs found their responsibilities growing over time to include other security-related functions in collaboration with the Coast Guard including port security grant reviews.

Assessing the state of public-private collaboration in 2011, the National Academy of Sciences of the National Research Council highlighted AMSCs as a success story:

> Concern with terrorism and the accompanying new funding opportunities led to the development of specialized homeland security partnership networks at federal, state, and local levels that were largely independent of networks already established by the traditional emergency-management agencies. Immediate concerns led to effective partnerships that addressed… port security (*e.g.*, *area security committees*)" (National Research Council, 2011).

Whereas the TWIC program was a singular nationalized component of a larger piece of seaport security related to access, no one entity owned the TWIC program, and thus the security logics were imposed on the private sector's economic logics to little avail. On the other hand, the Coast Guard's approach to AMSPs and the AMSCs resulted in logics integration. The private sector economic logics internalized parts of the security logics to form a hybridized logic.

A 2007 GAO report to Congress recommended additional federal guidance for ports to aid in disaster planning and recovery. According to the GAO, "[m]ost port authorities GAO reviewed conduct planning for natural disasters separately from planning for homeland security threats" (Government Accountability Office, 2007). Recognizing the efficacy of existing AMSCs, the report recommended using them as a forum for further discussion on the topic of disaster planning. Thus, the hybridized logic led to newfound roles based on the success of the institutional experiment. As a result, beginning in FY07 the Department of Homeland Security shifted the model of port security grant allocation. Based in large part on the success of the AMSCs' ability to successfully complete the port assessments and port security plans, the role of the AMSCs continued to expand.

Citing partnership with the private sector as essential to its maritime missions, a 2011 White Paper on the Coast Guard stated that partnership with the private sector led "to establish best practices, improve regulatory compliance, evaluate risk, report unusual or suspicious activity, and participate in exercises to improve readiness" (U.S. Department of Homeland Security, United States Coast Guard, 2011).

Additional examples of this hybridized logic can be found in the many maritime organizations and firms that followed a similar path of logics integration. On 9/11, the largest maritime evacuation in history occurred thanks to a flotilla of watercraft which responded to the tragedy and evacuated more than a half million people from Manhattan. Within months of 9/11, American Waterway Operators (AWO) convened a "meeting of senior leaders from industry, the Coast Guard, and the U.S. Army Corps of Engineers to discuss security measures needed to protect industry assets and the nation's critical maritime infrastructure" (American Waterways Operators, 2008). Then, in early 2002 AWO produced a "model vessel security plan for member companies to enhance vessel security procedures. When the Maritime Transportation Security Act became law in November 2002, AWO worked with the Coast Guard to transform its plan into one of the first Alternative Security Programs approved by the Coast Guard" (American Waterways Operators, 2008). In the ensuing years, the AWO was willing to work with the security logics blending into the economic logics originating from the private sector. Over time, the inherent economic logics of the private sector integrated with the public sector's security logics leading to a hybridized logic. Another way to see this integration of logics is comparing the AWO mission statements in 2008 and 2009. Prior to 2008 the AWO had had the same mission statement for years:

> The American Waterways Operators is the national trade association representing the owners and operators of tugboats, towboats and barges serving the waterborne commerce of the United States. Its mission is to promote continuous improvement in safety and environmental standards, the long-term economic soundness of the industry and the importance of waterborne commerce in the national transportation system (American Waterways Operators, 2008).

In 2009, a revised mission statement also included "protecting homeland security":

> The American Waterways Operators represents the people who own and operate the tugboats, towboats and barges serving the rivers, coasts, Great Lakes and harbors of the United States. AWO promotes the industry's value to the nation as a driver of the U.S. economy with a positive impact on the American quality of life, moving vital commodities safely, providing family wage jobs, reducing air and water pollution, relieving highway congestion *and protecting homeland security* (American Waterways Operators, 2009, emphasis added).

To be fair, however, not all terminal operators I interviewed consider the AMSC structure as perfect. The Director of Security at one major shipping company told me that

> [t]he AMSC committee in this port is completely *fugazzy*. It's completely rigged. It's a complete good old boy network. It's not that way at every port; it happens to be that way here. The port security grant funds that are normally awarded, I've been denied one for the last [number] years running. I haven't got anything. Majority of the money in this port goes to fund multi-NYPD… whole new fleet of harbor boats. FDNY. All tied into that government thing (Interview 15, 2016).

Still, while few interviewees thought poorly of the AMSC structure, many other interviewees discussed the benefits of the system. One of the primary benefits was the ability to focus dialogue on key issues amongst peers who may never have been in the same room, otherwise. The communications flow enabled both public and private sector actors to engage in policy recommendations not possible had they been working in isolation. For example, one maritime security official related the following anecdote.

> We were in an AMSC meeting about a month ago, [when] a lawyer in the New York port area who was involved with writing the TWIC reg; she put her hand up at the end when they were discussing/talking to the admiral about what we should push and she said, 'you need to push implementation of the TWIC reader' and so [another AMSC member] put [their] hand up and… [they] said with all due respect to madam counselor, she doesn't live with the implementation of this, [operators] do. And [operators are] going to say that her comments, albeit from her point of view are fine. But from an implementation of ports standpoint, [operators] do not want these regs implemented unless it helps with the security of that facility and with that you need to do a risk assessment… they need to understand that risk assessment is assessed before applicability is… and

> that's where it is, people who are not in operations making the rules thinking they are sound but they are not" (Interview 32, 2016).

Another port security director at a major seaport expressed a deep appreciation for the AMSC's integration of public and private sector logics when they explained that every port has an area maritime security committee where "a lot of info is shared at these quarterly meetings" (Interview 33, 2016). Beyond the AMSC, the facility security directors from various firms have begun meeting on a quarterly basis. Overall, the AMSC is more and more grant-oriented and there are lots of avenues for dialogue in the port (Interview 33, 2016).

As the AMSCs matured, the Department of Homeland Security decided to leverage these bodies for an expanded function pursuant with the evolving boundary conditions of involved logics. With increasing scrutiny on security expenditures, the Department of Homeland Security changed the allocation process for the Port Security Grant Program. Prior to 2007, "all port areas competed for one pool of grant funding" (Government Accountability Office, 2011). Beginning in 2007, grant allocations leveraged "fiduciary agents to help manage the PSGP at the local level and ensure that all port partners were incorporated in the grant planning and grant allocation processes… a field-level review process is conducted by the applicable Coast Guard Captain of the Port (COTP) in coordination with DOT, the Maritime Administration, and appropriate personnel from the Area Maritime Security Committee (AMSC)" (Government Accountability Office, 2011). In addition to reviewing port security grant applications, FEMA mandated that high risk port areas (see map in Figure 3.6) "develop and implement a Portwide Risk Mitigation Plan (PRMP). The primary goal of a PRMP is to provide a port area with a mechanism for considering its entire port system strategically

as a whole, and to identify and execute a series of actions designed to effectively mitigate risks to the system's maritime critical infrastructure" (Government Accountability Office, 2011). AMSCs were engaged to assist with management and review of these security planning processes and thus, the port security grants.

As of 2011, the Coast Guard "had organized 43 AMSCs. Each has flexibility to assemble and operate in a way that reflects the needs of its port area, resulting in variations in the number of participants, the types of state and local organizations involved, and the way in which information is shared" (Government Accountability Office, 2011). The original security logics intended to foster cooperation and communication with key port stakeholders through the AMSC process. However, as the economic logics regained dominance and the post-9/11 roles of the private sector were integrating security into the economic logics, the AMSCs evolved from a communications and trust building platform into a policy guidance, resource allocation and collaboration entity. Whereas the TWIC had been a nationalized security program overseen by the TSA, the AMSCs were a seen as a grass-roots collaborative effort that, while initially guided by the Coast Guard, took on a collaborative life of their own.

By 2013, most members of the maritime community agreed that the AMSCs had achieved their original stated goals although, as 9/11 receded, so too did active participation in the Committees. A comprehensive report was assembled by the Coast Guard regarding the AMSCs and lessons learned from the public private partnerships therein. Admiral Servidio, quoted above providing TWIC testimony, claimed "[i]n the decade since the first Area Maritime Security Committees were formed there have been significant threats – but no successful attack – in the Marine Transportation System. This

is a direct result of the hard work [the AMSCs] and the organizations they represent, have undertaken to assess risk, establish and meet standards, develop plans, coordinate operations and share information. Port areas… are more secure, resilient, and prosperous" (Servidio, 2013).

AMSCs were required by law to meet at minimum once per year. Routinized meeting schedules and increasing collaboration between AMSC members had led to a host of additional activities. In 2012, AMSCs "conducted 457 meetings nationwide" and conducted 129 Joint Agency training events (Servidio, 2013). The Coast Guard is divided into two major "areas": the Atlantic and Pacific, known colloquially as LANTAREA and PAC AREA, respectively. Figure 3.8 shows the scope of engagement across all AMSCs.

Interestingly, the 2013 Area Maritime Security Committee Annual Report mentions two challenges common throughout the various AMSCs: the cumbersome Port Security Grant Program and declining participation amongst AMSC members. "Reasons cited for declining support included the increased responsibilities of AMSCs, budget pressure, and the long distances some members must travel for committee meetings" (U.S. Coast Guard, 2013).

Citing the importance of trust amongst collaborators, the Coast Guard's efforts to develop partnerships between the public and private sectors were highlighted as a positive example. A 2011 study noted "important for community-level collaboration to consider how to familiarize those engaged with the needs and resources of other collaborators and how to build trust among them. There are examples of effective local

and regional collaboration led by DHS agencies that could be used as models. For example, the Coast Guard supports local private–public harbor-safety committees and regional area-security committees that bring together government, private, and nonprofit users of ports and waterways to collaborate on safety and security issues. The Coast Guard and the National Research Council's Transportation Research Board co-sponsor an annual conference for those committees" (National Research Council, 2011).

3.5 CONCLUSIONS

"A National Goal: No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures…" - National Goal established in 1998 by PDD-63.

Seven years after the aforementioned National Goal was established by Presidential Directive, many wondered if critical infrastructure was any more protected than it had been in 1998. A 2005 study seemed to predict the forthcoming economic salience, when it reminded its audience that the "broad support" for greater seaport security was a slippery slope and that "bringing commerce to a crawl in order to be completely safe carries its own serious economic consequences. Striking the right balance between increased seaport security and protecting economic vitality is an important and difficult task" (Wrightson, 2005). With prescience about the shifting logics, the report went on to predict that "the national dialogue on this issue is likely to focus increasingly in trying to determine what we are getting for our efforts and where we should invest the dollars we have" (Wrightson, 2005).

Thus, by 2007, the effects of 9/11 were still manifesting themselves in the ever-expanding panoply of security-related legislation and national strategies. However, the initial willingness on behalf of market logic-driven private sector entities to assist the government's efforts to shift the security paradigm was starting to wane. The full economic effects of the various security programs were being felt and as memories of the punctuated events of 9/11 receded, the full cost of the War on Terror (*e.g.*, Iraq, Afghanistan, Department of Homeland Security) coupled with the housing meltdown, set the country on a course for a prolonged recession. The economic logics of the private sector began to gain ascendency as a great deal of the burden for implementing national security strategies fell on the private sector. Not only as owners and operators of the critical infrastructure but as public sector assets were repurposed for other missions, the expanding role of the private sector in security enforcement raised serious issues about where on the balance sheet security investment would go. Firms were asking, "Was security an investment? Was security an asset or a liability?"

Questions also began to surface about the sustainable competitiveness for firms investing in security versus those that did not. On the one hand, if a security incident were to happen, those seaports who had prepared might fare better than those that did not. On the other hand, if a seaport did not prepare and nothing happened, it stands to reason that the seaport could have used fungible nature of unspent security dollars and invested them in other types of investment, marketing, and so on. As the national bill for security-related expenditures was moving into the tens of billions, some started asking, "Who is going to pay for this?"

The rising salience of economic logics was also a response to the broader macroeconomic effects as well. A 2008 study found that large, diversified economies had less impact from terror incidents than smaller economies when it came to evaluating the economic impact of terror events. However, 9/11 did not happen in a vacuum. Compounded with the macroeconomic effects of multiple armed conflicts and the economic downturn, we see the long-term effects of 9/11 were well-grounded in the immediate economic shocks. According to Sandler and Enders (2008) "[t]ransnational terrorist attacks often entail transboundary externalities: actions or authorities in one country impose uncompensated consequences on persons or property in another country. The spillover costs can result so that the economic effect of a terrorist event transcends the host country. [For example,] the toppling of the World Trade Center towers on 9/11 killed many British nationals and had ramifications for British financial institutions" (Sandler & Enders, 2008).

Another study "showed that 9/11 negatively influenced average return on stock markets globally. In fact, the 11-day cumulative average abnormal returns were larger on the London, Frankfurt, Paris, Toronto, Amsterdam, Switzerland, Italy and Hong Kong stock markets than on the NYSE following 9/11" (Chen & Siems, 2004). Chen and Siems (2004) also concluded that "U.S. capital markets are more resilient than in the past and recover sooner from terrorist attacks than other global capital markets. Evidence suggests that this increased market resilience can be partially explained by a stable banking/financial sector that provides adequate liquidity to promote market stability and minimize panic" (Chen & Siems, 2004). Government security expenditures, investment

in war materiel and extensive grant programs infused the post-9/11 economy with liquidity as well. This economic rebound is easy to see on Figure 3.9.

Further, Panel 1 in Figure 3.9 shows the growth of GDP following 9/11 and the temporary dip in consumer confidence in Panel 2 quickly rebounded perhaps due to a surge in patriotism (Sandler & Enders, 2008). We see the steady growth of durables consumption in Panel 3 coupled with the drop in the federal funds rate that spurred liquidity. The Panel 4 unemployment shows steady growth prior to 9/11; some economists think it would have continued to rise after 9/11 with or without the terror attacks (Sandler & Enders, 2008). Again, these positive macroeconomic signs probably sustained the security logics for a number of years as the private sector responded to public sector calls to prevent the next 9/11 with security expenditures. However, as the economic downturn took effect and the costs of the War on Terror continued to climb, the economic logics salience had begun in the private sector despite the public sector continuing as before with security logics-driven policies.

Eleven years after 9/11, Dr. Stephen Flynn criticized the public sector's investment in maritime security in that "as a nation, we continue to struggle with defining the appropriate role and investment that the federal government should make in managing our ongoing vulnerability to terrorism and other catastrophic risks on U.S. soil… For instance, the U.S. Navy has invested more in protecting the single port of San Diego that is home to the Pacific Fleet, than the Department of Homeland Security has invested in the ports of Los Angeles, Long Beach, San Francisco, Oakland, Seattle, and Tacoma combined upon which the bulk of the U.S. economy relies" (Flynn, 2012).

In the end, it was the effort to derive a suitable compromise between public and private actors in the implementation and enforcement of new rules that drove results. Thus, TWIC was never able to find this type of public-private partnership but AMSP, when a compromise was possible, did produce results. In particular, this need for compromise becomes apparent in the implementation stage of introducing new security-related policies. Imposing new security-logics on top of existing actors proved too expensive and challenging without shifting some responsibilities onto private actors.

More than a decade after 9/11, whereas the TWIC program continued to stumble, the AMSCs had proven their worth resulting in a sustainable model of security partnership.

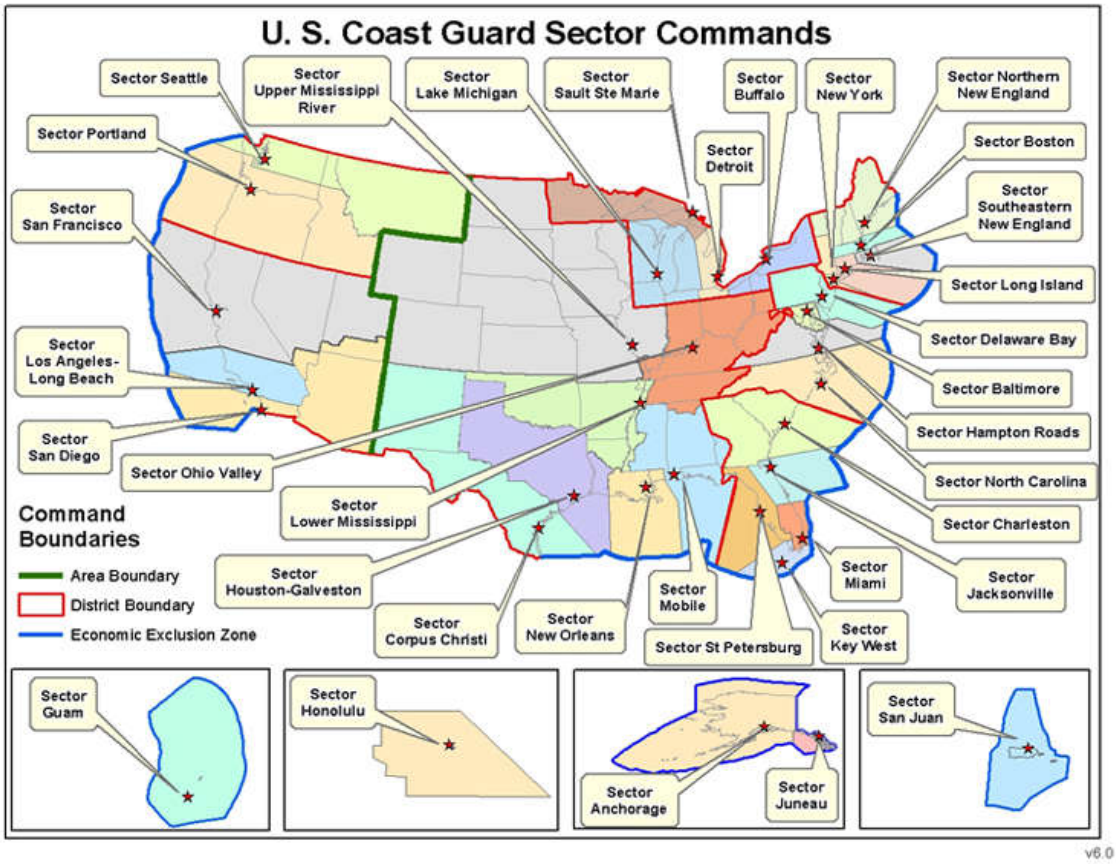
TABLE 3.1 (PART 1): PHASED-IN U.S. COAST GUARD CAPTAIN OF THE PORT ZONE COMPLIANCE SCHEDULE (REVISED FEB 19, 2009)

Oct-Nov 2008	Dec 2008	Jan-Feb 2009	Mar-Apr 2009
October 15, 2008 • Northern New England • Boston • Southeastern New England	December 1, 2008 • Long Island Sound • Charleston • Savannah • Jacksonville	January 13, 2009 • Hampton Roads • Morgan City • New Orleans • Upper Mississippi River • Miami • Key West • St. Petersburg	March 23, 2009 • New York
November 28, 2008 • Corpus Christi • North Carolina • Cape Fear River	December 1, 2008 • Buffalo • Duluth Detroit • Lake Michigan • Sault Ste. Marie	February 12, 2009 • Honolulu (with exception of American Samoa) • South East Alaska • Prince William Sound • Western Alaska	April 14, 2009 • Guam • Houston/Galveston • Los Angeles/ Long Beach • San Juan
	December 30, 2008 • Baltimore • Delaware Bay • Mobile • Pittsburgh • Ohio Valley • Lower Mississippi River • San Diego	February 28, 2009 • Puget Sound • Portland (Oregon) • San Francisco Bay	April 14, 2009 • American Samoa (within COTP Zone Honolulu)

Source: Government Accountability Office, 2009

TABLE 3.1 (PART 2): MAP OF U.S. COAST GUARD SECTORS / COTP ZONES

(NOTE: EACH SECTOR COMMANDER HAS A DUAL ROLE AS CAPTAIN OF THE PORT (COTP) FOR THAT SECTOR)



Source: U.S. Coast Guard, 2016

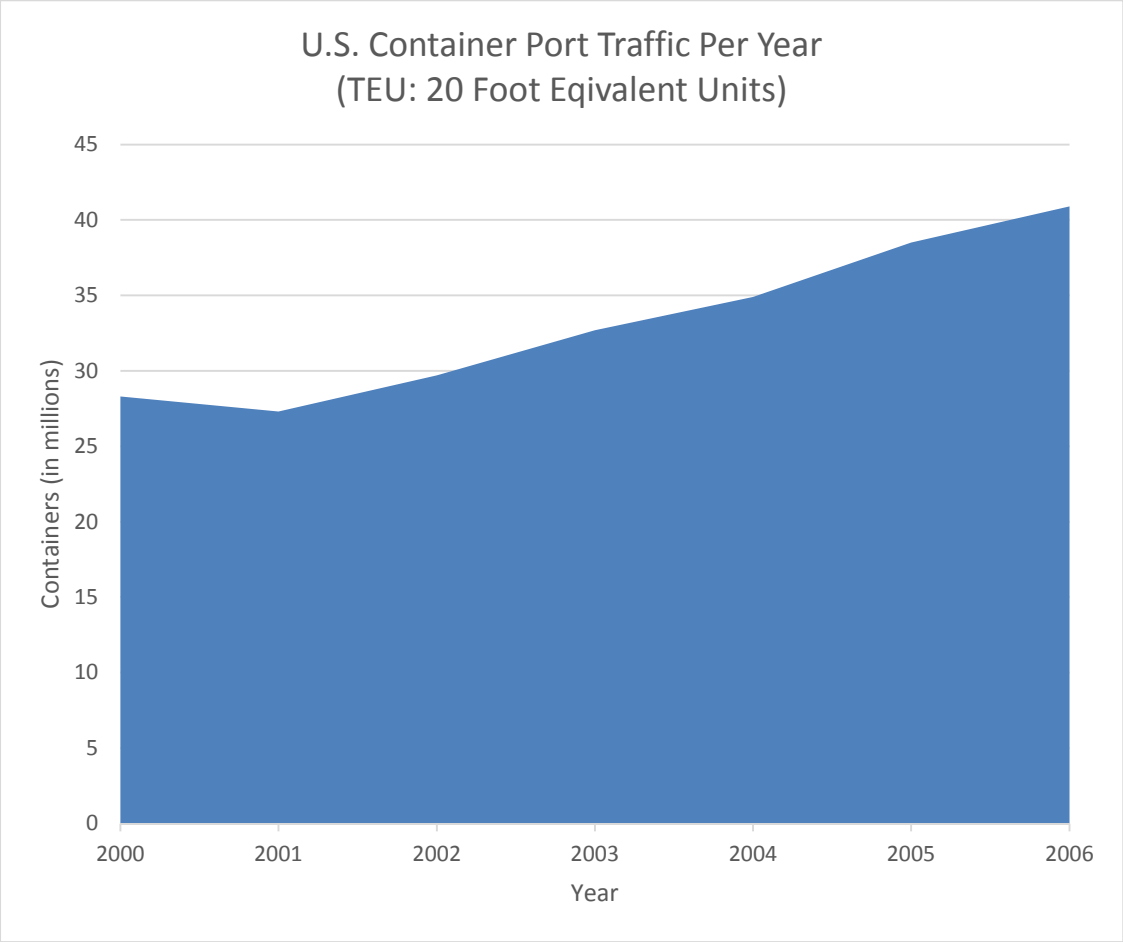


FIGURE 3.1: U.S. CONTAINER PORT TRAFFIC PER YEAR (TEU: 20 FOOT EQUIVALENT UNITS)

Source: The World Bank (2016).

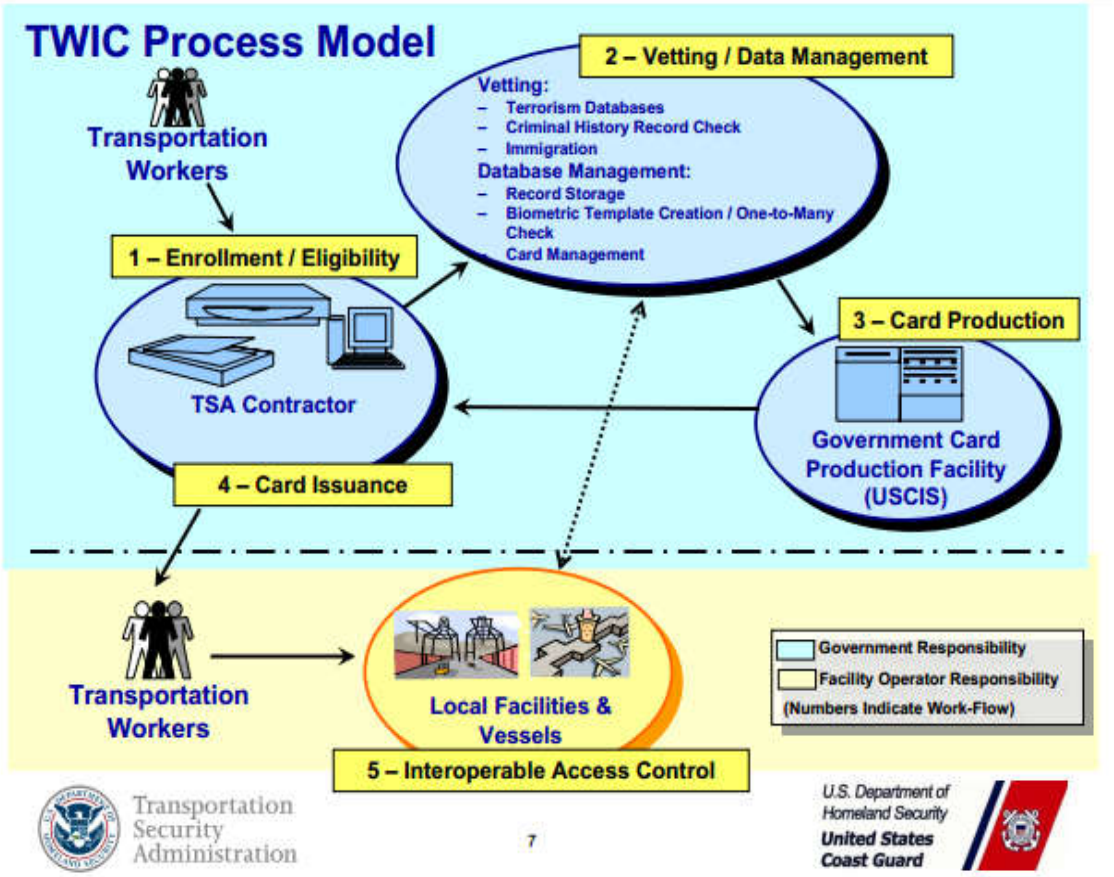


FIGURE 3.2 AREA MARITIME SECURITY PLANS: COLLABORATIVE BLENDING OF SECURITY AND ECONOMIC LOGICS INITIAL SUCCESSES

Source: U.S. Department of Homeland Security, Transportation Security Administration & U.S. Coast Guard (2006)

Date	Key TWIC implementation actions
November 2002	Enactment of the Maritime Transportation Security Act of 2002, which required the Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics to control access to secure areas of maritime transportation facilities and vessels.
August 2004 through June 2005	As part of its prototype testing, TSA—through a private contractor—tested the TWIC program at 28 transportation facilities across the country.
August 2006	TSA decided that the TWIC program would be implemented in the maritime sector using two separate rules. The credential rule covers use of TWICs as a credential for gaining access to facilities and vessels. The second rule, the card reader rule, is planned to address the use of access control technologies, such as biometric card readers, for confirming the identity of the TWIC holder against the biometric information on the TWIC.
October 2006	The Security and Accountability For Every Port Act directed the Secretary of Homeland Security to, among other things, implement the TWIC program at the 10 highest-risk ports by July 1, 2007, and to conduct a pilot program to test TWIC access control technologies, such as TWIC readers, in the maritime environment.
January 2007	TSA and the Coast Guard issued the credential rule requiring worker enrollment in the TWIC program and TWIC issuance. The Transportation Security Administration also awarded a $70 million contract to begin enrolling workers and issuing TWICs to workers.
July 2007	The Coast Guard issued guidance on how the maritime industry is to comply with the credential rule and how the Coast Guard will implement TWIC compliance efforts.
June 2008	As part of the TWIC reader pilot, TSA issued an agency announcement calling for biometric card readers to be submitted for assessment as TWIC readers.
August 2008	TSA initiated the TWIC reader pilot testing, starting with the initial capability evaluation of TWIC readers.
October 2008	Phased-In TWIC compliance began at Captain of the Port Zones' in Boston, Northern New England, and Southern New England on October 15, 2008.
April 2009	On April 15, 2009, all Captain of the Port Zones nationwide began compliance with TWIC requirements.

FIGURE 3.3: KEY TWIC IMPLEMENTATION ACTIONS 9/11 TO 2009

Source: Government Accountability Office, 2009

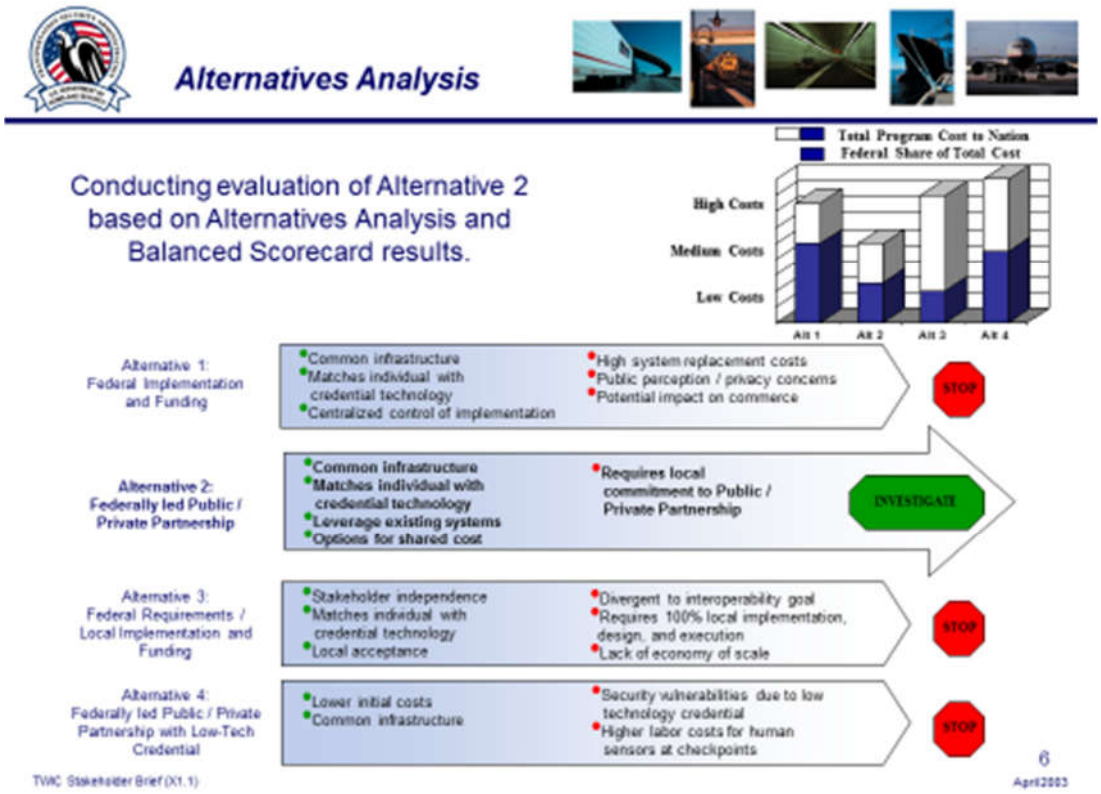


FIGURE 3.4: INITIAL EVALUATION OF TWIC IMPLEMENTATION ALTERNATIVES

Source: TSA PowerPoint Briefing, April 2003

Requirement	Description of requirement
Transportation workers	Individuals who require unescorted access to secure areas of maritime transportation facilities and vessels, and all merchant mariners, must obtain a TWIC before such access is granted.
Fees	All workers applying for a TWIC will pay a fee of $132.50 to cover the costs associated with the TWIC program. Workers that have already undergone a federal threat assessment comparable to the one required to obtain a TWIC will pay a reduced fee of $105.25. The replacement fee for a TWIC will be $60.
Access to secure areas of maritime facilities and vessels	By no later than April 15, 2009,[36] facilities and vessels currently regulated under the Maritime Transportation Security Act must change their current access control procedures to ensure that any individual or merchant mariner seeking unescorted access to a secure area has a TWIC.
Newly hired workers and escorting procedures	Newly hired workers who have applied for, but have not received, their TWIC, will be allowed access to secure areas for 30 days as long as they meet specified criteria, such as passing a TSA name-based background check, and only while accompanied by another employee with a TWIC. Individuals that need to enter a secure area but do not have a TWIC must be escorted at all times by individuals with a TWIC.
Background checks	All workers applying for a TWIC must provide certain personal information and fingerprints to TSA so that they can conduct a security threat assessment, which includes a Federal Bureau of Investigation fingerprint-based criminal history records check, and an immigration status check. In order to qualify for a TWIC, workers must not have been incarcerated or convicted of certain disqualifying crimes must, have legal presence or authorization to work in the United States, must have no known connection to terrorist activity, and cannot have been adjudicated as lacking mental capacity or have been committed to a mental health facility.
Appeals and waiver process	All TWIC applicants will have the opportunity to appeal a background check disqualification through TSA, or apply to TSA for a waiver of certain disqualifying factors, either during the application process or after being disqualified for certain crimes, mental incapacity, or if they are aliens in Temporary Protected Status. Applicants who apply for a waiver and are denied a TWIC by TSA, or applicants who are disqualified based on a determination that he or she poses a security threat, may, after an appeal, seek review by a Coast Guard administrative law judge.
Access control systems	The Coast Guard will conduct unannounced inspections to confirm the identity of TWIC holders using hand-held biometric card readers (i.e., TWIC readers) to check the biometric on the TWIC against the person presenting the TWIC. In addition, security personnel will conduct visual inspections of the TWICs and look for signs of tampering or forgery when a worker enters a secure area.

FIGURE 3.5: JANUARY 2007 TWIC RULE HIGHLIGHTS

Source: Government Accountability Office, 2009

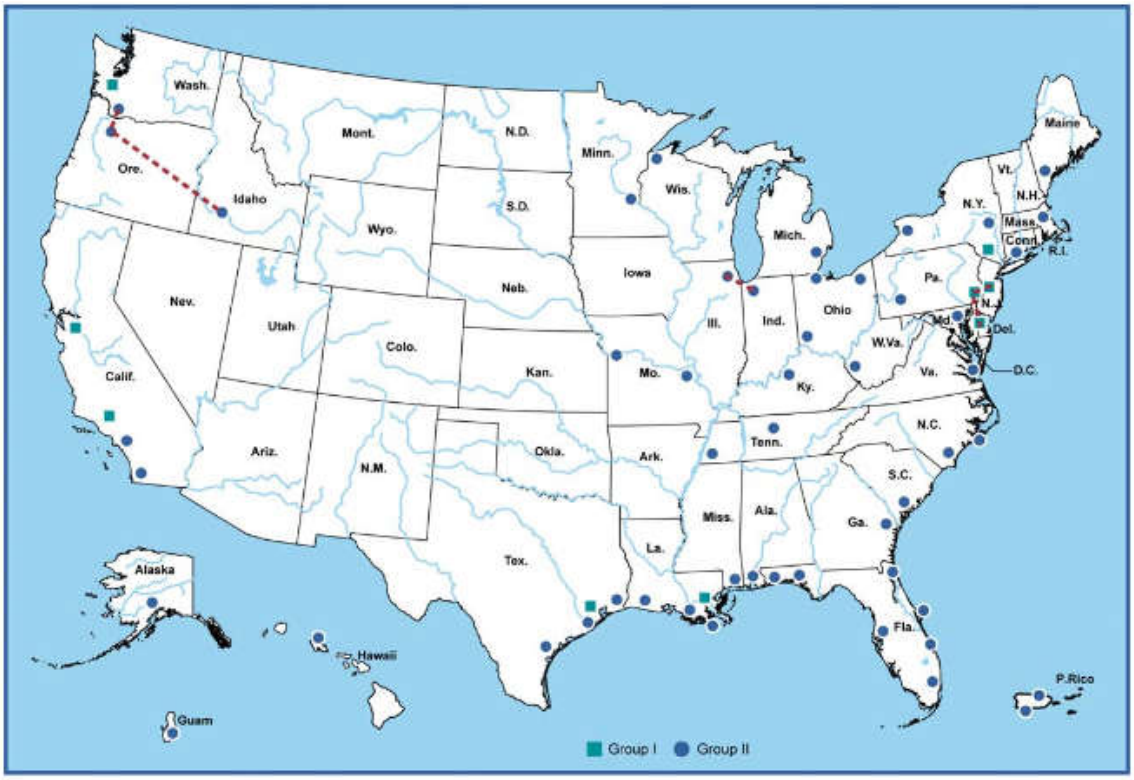


FIGURE 3.6: LOCATION OF HIGH RISK SEAPORTS (GROUP I AND GROUP II PORT AREAS)

Source: Government Accountability Office, 2011

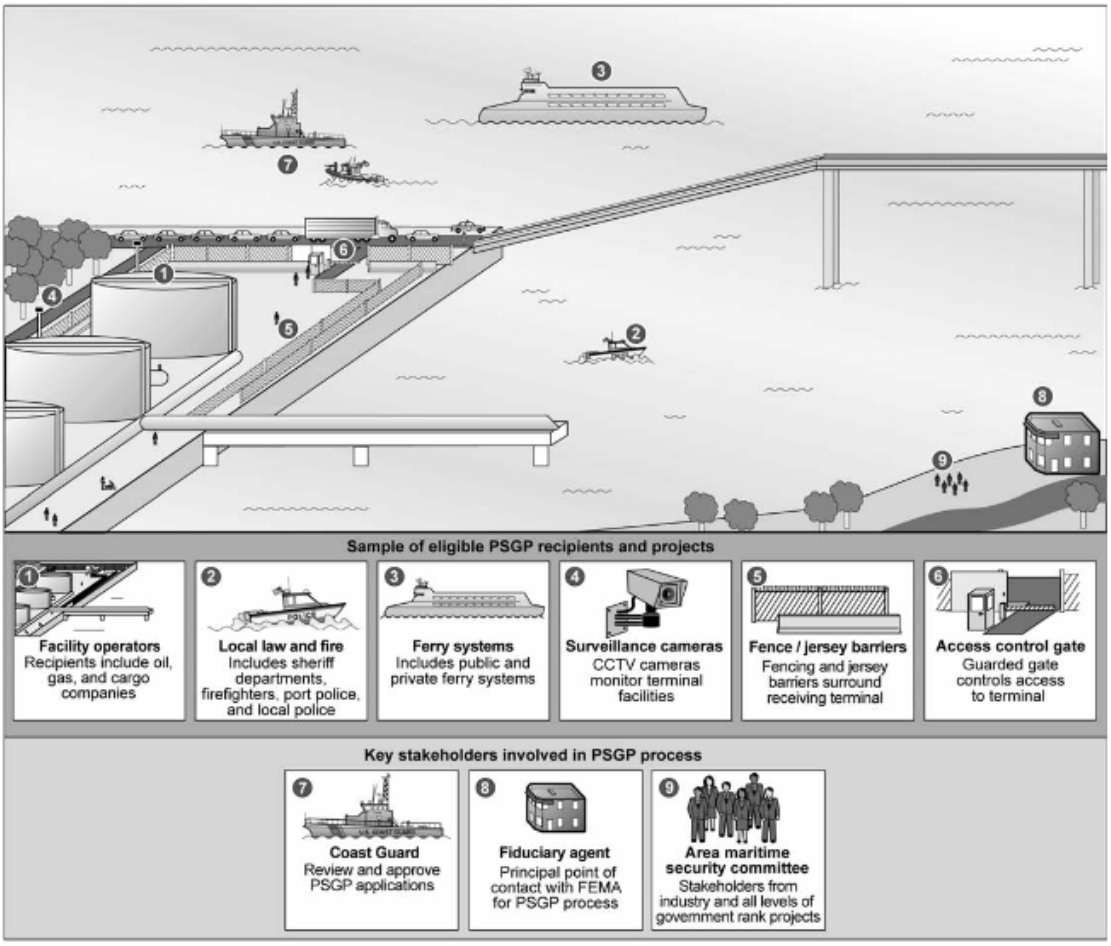


FIGURE 3.7: SAMPLE PORT AREA SHOWING ELIGIBLE PSGP RECIPIENTS AND PROJECTS, AND KEY PORT STAKEHOLDERS INVOLVED IN THE GRANT PROCESS

Source: Government Accountability Office, 2011

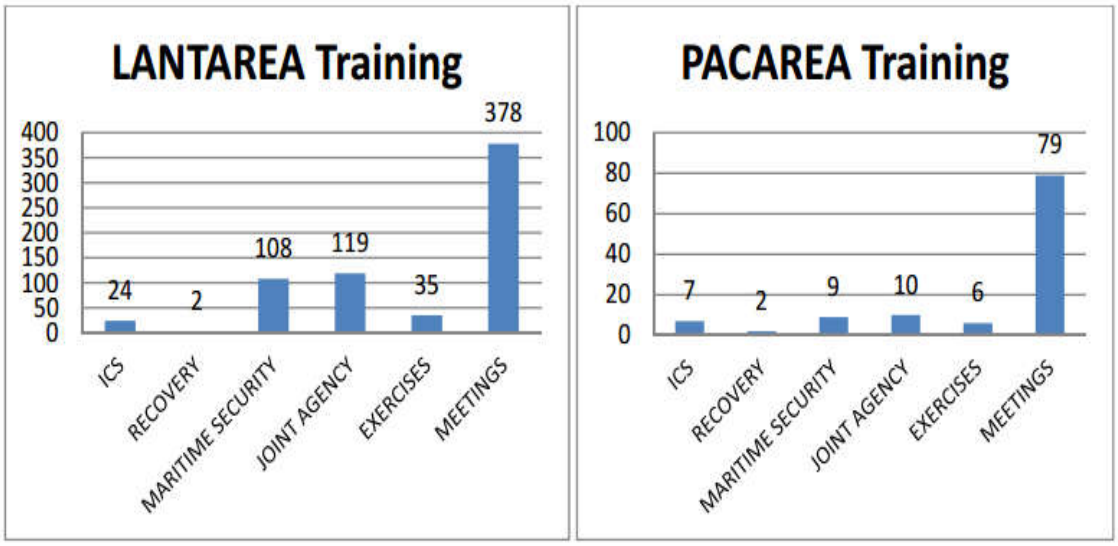


FIGURE 3.8: BREAKDOWN OF AMSC TRAINING AND MEETINGS

Source: Servidio, 2013.

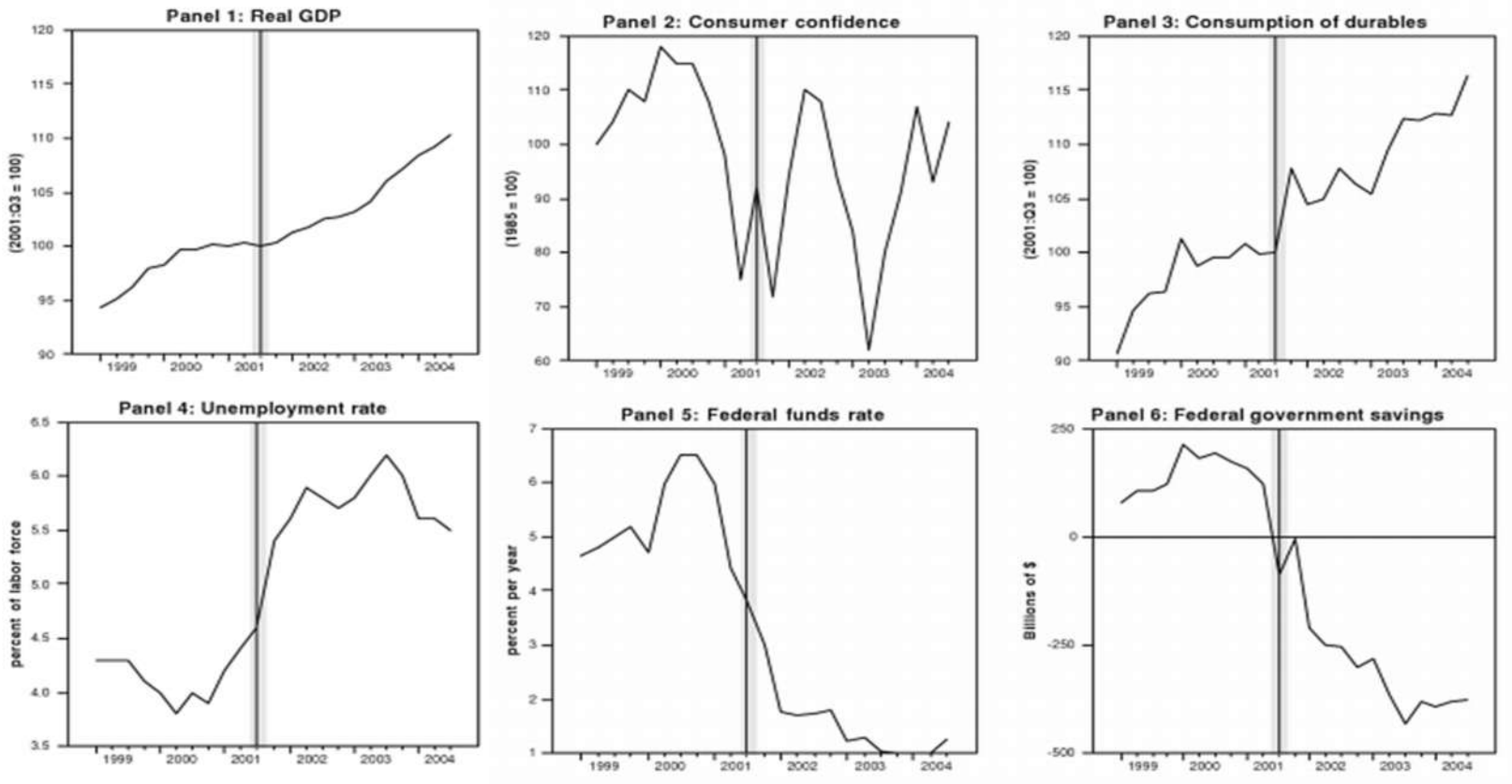


FIGURE 3.9: MACROECONOMIC VARIABLES AND 9/11

Source: Sandler and Enders, 2008

CHAPTER 4: INSTITUTIONAL LOGICS AND THE SHAPING OF PUBLIC-PRIVATE BOUNDARIES

"There's been an evolution in the relationship between the federal government and the private sector since 9/11 that was rooted in responsibility. The federal government had a responsibility to protect and defend the people of the United States. As a result of 9/11, the fact that we missed a whole bunch of dots that we didn't connect, the government took it upon itself – accepted responsibility – for our inability to detect and prevent 9/11 from happening… Now we have a whole bunch of folks just waiting for the government to tell them what to… you can't have the answers if you don't have the questions… the question's come from people who know their communities best. It's what Tom Ridge had to say, 'The homeland is not secure until the hometown is secure.' Over time, it has devolved to the government knows best. And we know that is not true." - Interview 43, 2016

Throughout this study, I have shown how the increasing salience of the security logics following a transnational terrorist attack interacts with existing institutional structures and beliefs to shape substantive change over time. As the opening quotation illustrates, my research moved beyond theories that look at the intersection of business and security as separate institutional domains in which issues of public security are solely left to government actors implementing an ideal type security logic. That is, it became increasingly apparent that an explanation of the effects of security on the governance of critical infrastructure like seaports could not be fully understood only by exploring the activities or strategies of those actors that sat within the political domain, such as the politicians and civil servants that staff the U.S. Congress or the U.S. Department of Homeland Security. Instead, economic logics and actors clearly entered the picture during efforts to implement new ideal type security logics on existing economic social

structures. Throughout my analysis of the implementation of the Transportation Worker Identification Credential (TWIC) and Area Maritime Security Plans (AMSPs), I demonstrate the emergence of "blended" or "hybrid" outcomes that sit at the intersection between security, political and economic logics, allowing for the possibility that outcomes may emerge that do not fully fit within in any ideal type institutional logics.

To advance these ideas, I posed the following research questions to guide my efforts in a grounded methodology to extend the literature of the role of terrorism in shaping the long-term relationship between business and security:

1. What are the long-term consequences of a punctuated transnational terrorist event on the institutional environments of business?
2. Specific to a major terror related event, how do security-based logics interact with existing political and economic institutions to produce change?
    d. What is the role of the private sector in implementing security-based institutional changes?
    e. How much do security-based institutional change strategies influence the long-term institutional environment of business?
    f. How can security-based institutional change efforts be evaluated in term of long-term impact? What explains differences between transformational and incremental institutional change?

In this final section, I return to addressing each of these questions in light of the lessons learned from my analysis of long-term institutional change in seaport governance and access following the September 11, 2001 terrorist attack.

4.1 The Long-Term Effects of a Transnational Terrorist Attack on Security-Based Institutional Change: Rethinking Public-Private Boundaries

This study relaxed an assumption found in many earlier firm-level studies of logics that the boundaries between different institutional domains are themselves fixed or static over time. As a result, I explored the intersection of alternative logics as a force of long-term institutional change. Institutions change as alternative logics, and the societal actors assigned to protect them, come together to create practices that reflect a compromise or blending of existing logics that pushes joint strategies and outcomes in new directions. Thus, in contrast to studies that delve into *ideal types* in isolation from other institutional logics, this dissertation looked at logics in action as a force of long-term substantive change.

From this perspective, the issue in understanding change processes was not simply to identify why some members of society might call for a new type of institutional change, such as strengthening the rules that protect the security of critical infrastructure organizations. I also identified the ways that prescriptive calls for new directions interacted with existing institutional logics and structures in shaping realized outcomes. For instance, Holm's (1995) basic insight that "[n]ew institutions are not created from scratch but are built upon older institutions and must replace or push back preexisting institutional forms" (Holm, 1995) provided insight into the Coast Guard's development of the Area Maritime Security Committees (AMSCs) that were built off previous experience with Area Safety Committees. According to Purdy and Gray (2009), ideal type institutional logics are not deployed fully formed but become part of the toolkit of

actions as various individuals come to mobilize to try to enact change within preexisting networks of interests, actors and beliefs. Again, we found evidence of this with the emergence of the security logics after 9/11 and how the various actors mobilized to enact change and how those actors reacted to change.

Purdy and Gray (2009) advanced research into examining institutional hybridity by proposing an initial typology to categorize the way in which a new logic may come to influence an existing institutional field: transformation, grafting, bridging and exit. We found evidence of these through the field research and have developed a clearer understanding of the variance resulting from the different approaches inherent in the various typologies. *Transformation* referred to situations in which a desired new institutional logic came to replace existing practices; others call this a "replacement" outcome, as one institutional logic is simply replaced by another (Thornton, Lounsbury & Ocasio, 2012). This was clearly evident when the TWIC was introduced and the new actors, the Department of Homeland Security and the Transportation Security Administration (TSA), sought to nationalize existing access strategies with implementation of a national transportation worker identification credential.

Purdy and Gray (2009) identified another outcome of conflicting institutional logics as *grafting*. Rather than replacing existing practices, the new logic comes to be placed at the periphery of existing dominant logics. The new logic does not transform the core of the existing system but instead becomes incorporated within existing logics without changing core beliefs or practices. To a limited extent, this is what happened with the Coast Guard's installation of AMSCs and their successful implementation of security assessments and AMSPs. However, we discovered that the successful

implementation of these was not fully and accurately explained by the "symbolic" implementation illustrating what Purdy and Gray (2009) describe as grafting in which new ideas are ceremoniously accepted for external legitimacy but do not penetrate into the substantive activity of the existing institutional structures. Investigating further, we realized that while grafting started to tell part of the story, it was not the whole story. Thus, we turned to Thornton, Ocasio and Lounsbury (2012) who further elaborated on these different categories of institutional hybridity. Under the category of transformational change, they include the cases of replacement and blending as Purdy and Gray (2009) proposed, but also introduce the concept of a segregated case of institutional hybridity, where both logics exist but remain fully separated from each other in their implementation. Again, however, the success of the AMSCs and AMSPs were not exactly the right fit as the two logics did not so much coexist as they did form something new.

This is where the York, Hargrave and Pacheco (2016) study built on these concepts in a further elaboration of the role of logics in shaping both the processes and outcomes of institutional change. These authors differentiate between *hybridization* and *blending* as ways in which distinct logics co-inhabit a similar institutional field. They propose that logic hybridization "differs from blending [in the Thornton, *et al.*, 2012 usage] in that the goals of incompatible logics are integrated as complementary; they do not merely coexist. … [Instead], hybridization processes change the relationship between incompatible logics, eventually leading to a new hybridized logic that integrates the incompatible logics." That is, York, *et al.*, (2016) suggest that hybridization reflects an outcome in which new logics can emerge that encompass elements of both new and

existing beliefs and practices. And this, we believe, is where our research points as the ideal situation for understanding the long term effects of a punctuated transnational terror attack on long-term institutional change. The issue that emerged, and is still not yet fully resolved is how to rethink public-private boundaries in the face of new security concerns. Who is responsible for security? Who governs the day-to-day implementation of new security initiatives and plans? And who pays for more secure infrastructure organizations?

These questions relate to the additional issues that I raised in my initial research questions. The role of the private sector, as well as differences between transformational and incremental change, arose not from the desired goals espoused in legal plans or Department of Homeland Security strategies but instead within the efforts to turn ideal security logics into actual organizational practices. To further address these issues, I look first to the lessons of the TWIC implementation and then to the AMSP to further ground our understanding of the long-term institutional effects of transnational terrorist events on long-term institutional change.

4.2 Building Theory from the TWIC Program: Limits to a Replacement Strategy of Institutional Change

The TWIC program demonstrates the challenges and limitations of a limited replacement strategy of institutional change. With little consideration beyond the security logic that controlling access on the seaport is a worthwhile endeavor, partial implementation of the logic translated into actual practice results in governance challenges, implementation questions, and disagreement over division of responsibility,

resource allocation, as well as perhaps even ethical and legal liabilities. The TWIC process was originally intended to be implemented at all seaports within a couple of years and then to be institutionalized across all aspects of the U.S. transportation system. As it stands, actual implementation has fallen short of the intended design at nearly every step of the process.

An explanation of the relatively failed implementation of TWIC can be illustrated when we take the abstract ideal of security logics and then consider what it means in practice, *e.g.*, to the guard hired to work in the port terminal guardhouse. The guard has been hired to verify data on the identification cards but at the same time, a terminal with thousands of tractors hauling freight can ill afford multiple minutes per driver being delayed at the guard checkpoint. Thus, the security guard understands that full compliance with the security logic would result in unsustainable backlogs of vehicles and goods. The resultant delay has a personal effect on the guard when he realizes that the lack of commitment from institutions to ensuring 100% TWIC compliance is weighed against competitive pressure to ensure efficiency of the containers in and out.

Thus, in practice, we end up with something different than the original ideal (and abstract) security logic. These issues of building new implementation structure are particularly apparent in comparison to the TSA takeover of airport security. One only has to attempt boarding an aircraft – and wait in the security line for an extended period of time – under the nationalized security provided by TSA to realize that TSA has determined a relatively high friction threshold to be an acceptable exchange for thorough inspection. That is, the security process is designed to be thorough, not efficient or customer friendly. Thus, the average TSA worker surely views his or her function

differently from the seaport guard considering the personal effects of 100% compliance with the security logic. Again, in this context, the seaport guard has 5000 trucks waiting to enter the check-point, while commerce must flow and ships have schedules. Seaport competition with other seaports is measured, in large part, in terms of efficiency and the ability to keep cargo and shipping on or ahead of schedule.

Efficient passage through the seaport checkpoint is wholly different from the TSA passenger model at airports. However, it is clear from this scenario that the TSA agent does not have to contend with the economic logic that includes efficiency and customer service. In contrast, the guard implementing the TWIC at seaports remains employed by the terminal owner, not the government. In this case, the experience of conflicting logics is quite different, as the desire to keep the terminal running in a timely and efficient manner is likely to remain more salient than putting in the time to protect against all forms of potential security threats.

One inconsistency with partial nationalization of the TWIC program is that while the burden of enforcing TWICs has clearly been transferred to private sector organizations and their guards manning access gates, it is not a shared burden amongst individual TWIC holders beyond the designated security force. Unlike airport employees, individual dockworkers beyond the security detail have no particular incentive to ensure TWIC compliance amongst other individuals present. Ideally, access is a layered defense strategy wherein both individuals and organizations collectively enforce adherence to compliance. Whereas holders of airport security cards are held accountable for security breaches that they fail to address, the TWIC has no such provision. For example, a security director for a port authority told me that little

responsibility is born by other individual TWIC holders for everyday security lapses: "We had an incident where an emotionally disturbed individual walked across the dock, past numerous longshoremen, up the ramp of RORO [Roll On/Roll Off vessel] and then made way to Master's couch. When discovered, he told everyone how he got there… but in aviation world, all those longshoreman would have been held responsible for letting him walk by… We have spent all this time and energy on a national credential and it is still just a flash pass" (Interview 23, 2016). Similar comments about the lack of enforcement of TWIC are repeated in the interviews presented in the previous chapter.

In terms of theoretical insights, I propose that a critical difference exists between the role of TSA in the case of airport and seaport security. In the airline industry, the TSA took over both the design and implementation of the program. Yet in ports, the TSA (with some division of labor from the Coast Guard) took over the design but not final implementation, maintenance and enforcement. Thus, the security logic was limited to the TSA and Coast Guard and then competed with the private sector economic logic for implementation and the resource allocation necessary to utilize, maintain and enforce the program. This resulted in new governance changes for the private sector with respect to logics that they did not own or have much of an opportunity to shape/manage.

Although the intention at seaports was the same as for airports – that is, access control for improved security – the massive infusion of resources and investments required for nationalization were not made available for seaport security. In the latter case, the replacement strategy failed to leverage existing trusted agents (*e.g.*, the Coast Guard, existing security protocols) and instead introduced another level of uncertainty with the introduction of the TSA as a preliminary decision-maker and implementer of the

program. Considering airport security, wholesale investment of the security logic as evidenced by nationalization (*e.g.*, massive investment) replaced the need for a collaborative approach and provided the TSA with a degree of legitimacy to ensure immediate compliance with new security directives.

We thus draw the following conclusion from a comparison of the airline and seaport experiences: a public sector replacement strategy requires a massive infusion of resources and investments to ensure that the new program is fully nationalized, similar to what happened with TSA and airports. In the absence of such a large and prolonged investment, then it is significantly less likely that a replacement strategy is likely to work to fully achieve its original objectives.

A corollary to this argument about the inherent limitations of a full-scale replacement strategy toward security is that new security programs that are not fully nationalized must– at least in part –infuse the security logic within existing economic structures. Arguably, the most obvious places to see the interaction between the security and economic logics is at border control points. After a major terror incident, the long term brings focus to these borders. Thus, visa regimes become more difficult, migration becomes a larger issue (both politically and economically), and both sides of the political spectrum draw closer in terms of tighter border control. Unlike airports, however, which have an easily discernible footprint that enables construction of a fence perimeter that is relatively inexpensive and easy to enforce, other border points are less easy to fully comprehend. Thus, the sprawling nature of seaports and their sheer size of some land borders make these border points much more difficult to easily discern and defend.

And yet, seaports as organizations have always had some type of security logic inherent in their being. Prior to 9/11, there was infrastructure at seaports designed to enhance some elements of security (albeit more focused on criminal activity like theft than counterterrorism) and thus designed to keep goods in rather than terrorists out. This bridging leads to repurposing of existing institutions as well as creation of new venues for collaboration, as exemplified in repurposed nature of the AMSCs to introduce new security procedures following 9/11. I now turn to the lessons learned from this experience in more detail.

4.3 Building Theory from the Area Maritime Security Plans/Facility Security Plans: Long-Term Change through Blended Institutional Logics

The juxtaposition of the two different strategies for implementing seaport security programs provide us with variation in the primacy of logics and thus, their ultimate effectiveness measured by actual institutional change (in this case, enhanced security). Whereas the TWIC program was designed to manage access to the seaports, the AMSPs and the Facility Security Plans (FSPs) were ultimately about determining variations of accessibility. Simply entering the hypothetical seaport gates with a TWIC was not a blanket pass to travel anywhere. Rather, the TWIC was intended to provide a degree of assurance that the holder was a trusted agent from a security perspective, but it was the overarching AMSP and the individual FSPs that delineated who was allowed access in various parts of the facility/terminal/seaport. This process highlights the long term institutional change resulting from blending institutional logics.

Specifically, the economic logic was given the opportunity to influence and even craft the boundary conditions of the security logic. The institutional changes sought with the AMSPs and the FSPs were increased security of seaport areas deemed to be particularly sensitive or high risk of penetration and exploitation by those with ill intent. The security logic manifested itself in the introduction of the program and the basic guidance and advice available from the public sector trusted agent (the Coast Guard). But, the ultimate design of the plan and its integration with day to day operations and activities was recognized to be necessarily, and perhaps infinitely, flexible as seaports, and more specifically, individual tenants within seaports, each have their own unique functions, operations and facilities. Thus, for example, hybridizing the logics enabled petrochemical terminals to develop security plans unique (and different) from large passenger cruise ship terminals. This blending and eventual hybridization of logics resulted in more sustainable and effective security outcomes. Whereas real security benefits of the TWIC program continue to be elusive, fully implemented and operationalized FSPs ensure at least a higher degree of security than before the program was implemented. An additional benefit of this hybridization of logics had ancillary benefits as well with increased trust, dialogue and collaboration into other aspects of the seaport.

This repurposing looks less like a government takeover and more like a new partnership in reshaping public-private boundaries to protect security. Through the partnership, the public and private sectors work in tandem to develop security committees built from pre-existing safety committees. Likewise, the partnership enables the firm to develop its own security plans while a long-term trusted agent seen more as a partner

(*e.g.*, Coast Guard Captain of the Port) reviews and approves them. Completely different from the airline industry experience, the seaports see real changes in both physical security and in governance structure as emphasis is placed on private sector protection of its own assets and development of its own plans to then organize that protection.

Thus, my research underlines the distinction between a centralized versus decentralized strategy of security-related institutional change. Unlike the centralized approach taken through the TWIC implementation, the decentralization/partnership approach taken through the AMSPs led to the more successful development of security plans by seaport stakeholders and the relatively successful implementation of those plans in a timely fashion. Existing institutions were repurposed and assets were reassigned or newly created to meet new conditions. In the following sections, I look to the implications of such a blended institutional approach to understanding and enacting security-related institutional changes from both a private and public perspective.

4.4 Implications for Private Actors: The Corporate Social Responsibilities of Security

One of the unique aspects of this study is considering the spillover effects into other industries and other environments from the punctuated terror attack. Thus, one insight we receive from considering the long term effects of terrorism beyond the boundaries of the single firm is an awareness for the expanding security role well beyond the direct target of the original 9/11 attack. We find that these spillover effects are transnational in scope in that codification of these new firm responsibilities, coupled with pressure from both political and security logics as well as the firms' natural inclination to

at least minimally protect itself, result in newfound roles for the private sector. It is one thing for a seaport terminal to hire a night watchman to keep an eye on the warehouse and something else entirely for the public sector to require the firm to serve as the frontline check of nationalized identification credentials and then expect the firm to detain transgressors until the public sector agents arrive to investigate.

And so, security becomes akin to other social responsibilities and the expense of additional security measures are seen by the public sector as investments in the public good even if counted on the expense side of the firm's balance sheet or as potential liabilities if the firm failed to live up to its newfound responsibilities. This becomes even more pronounced for firms owning and operating critical infrastructure. The public good guaranteed by the continued existence of that infrastructure may become a liability if the firm has not properly prepared a resilient defense against a terror attack or even being caught in the cascading effects of a terror attack in another industry that happens to impact the firm.

Thus, while the security logics thrust into the spotlight after 9/11 were recognized immediately within the aviation industry we also see a slow extension of these implications over time across other sectors. Perhaps not as quickly or with as much investment as the aviation industry, but we do see extensions of corporate social responsibility across other critical infrastructures and, in the case of this study, the maritime industry. However, this extension of corporate social responsibility is not without limits. Over time we see strong private sector frustration with various security programs including the TWIC.

Often times the private sector desired clearer definitions and boundaries and a more clearly articulated delineation between the security roles of the public and private sector. In particular, a strong implication of this research for private actors is to pay increasing attention to the role of the private sector in determining those delineations or else these costs may be placed on economic actors, perhaps even inefficiently as seen in the case of the TWIC. It is this intersection of public and private concerns over security that can contribute to the existing business literature on security that looks solely at this issue from a firm-level perspective of political risk and legitimacy. As previously mentioned, Czinkota, Knight, Liesch, and Steen (2010) suggest that firm incentives to manage terrorist events include the activity of managing and sustaining its efforts to establish its legitimacy among relevant constituents or else face potential new costs to government oversight stemming from the introduction of new security-related improvements. In particularly, these authors suggest that "new measures such as the… Maritime Transportation Security Act… have imposed tens of billions of dollars in compliance and other costs on private sector firms" (Czinkota, *et al.*, 2010, 831). Our case study illustrates the ways in which such spiraling costs can be imposed on private actors, particularly those tied to the running of critical infrastructure.

A contribution of my research is to situate these firm concerns within a broader institutional context. The debate over public-private boundaries takes place within a broader politicized field that includes political, security and multiple types of economic agents, thus introducing an inevitable period of uncertainty for any economic actor wishing to hope for a clear and defined set of responsibilities that can be implemented with clear costs and consequences. There is on-going uncertainty over the fate of TWIC.

For instance, as recently as March 2016, the Coast Guard published the long-awaited guidance on card reader requirements for seaports. Afterward, one senior leader at a national trade association told me that his organization would support expansion of the TWIC but that its future was in doubt. "We definitely see value in the program… it's all kind of gone into a black hole and now it's stuck" (Interview 16, 2016).

The historical narrative of long-term institutional change at seaports suggests that the study of corporate security responsibilities are presently becoming renegotiated and discussed by both public and private actors. For instance, one corporate interviewee in my research study captured this need for additional understanding of the changing public-private interface in the following manner:

> What we need to do… is recalibrate the public perception of what security is and also the private sector's view of what security is. I dismiss the idea that these are tradeoffs. That you have to [trade] security with efficiency. That you have to [trade] security with privacy. There are tensions here that have to be worked out but it is not a zero sum game. That's how it has often been portrayed so it often reinforces the clash of norms that you are looking at here. There are important opportunities for these things to be mutually reinforcing. Part of it is stepping back and looking at what is the end we are trying to achieve. What are trying to secure? For many in the law enforcement perspective and the national security side that is easy, we have to keep loss of life to a minimum or keep any risk of violence in check. We have to do whatever it takes to prevent the loss of life or destruction of property. And these are the protective measures one must do to mitigate those risks.
>
> But what is misguided about that is that it misunderstands the role that the maritime transportation industry and other critical infrastructure sectors provide which is – they are not just assets that pose risk – they are systems and networks that provide enormous benefits that are central to the way our society functions and if we do not have mobility and the ability to connect with markets around the world, the United States with just 5% of the world's population, obviously a much larger share of the world's economic activity, is largely an island nation when it comes to how the global economy is working today. And its umbilical cord to the economic life or the international community is the maritime transportation system (Interview 44, 2016).

Moreover, his recommendations to accomplish this goal of rethinking public-private boundaries also resonate with the conclusions of this study to examine solutions at the intersection of the public and the private rather than through the lens of any single logic. This framing of seaports as part of a larger system is absolutely essential to the long-term development of effective and sustainable governance structures. Reflecting on the cascading effects of critical infrastructure failures, seaports in the modern age have never been more important both from a security perspective and an economic perspective. Understanding seaports as part of an extended system also emphasizes the fallacy of a replacement logic approach to security. A complex system requires the integration that hybridity can introduce. This integration, then, is exactly where the hybridized logics can serve to foster stronger public-private partnerships.

This gets at the very essence of the primary lessons from this study. The shaping of public-private boundaries is essential to successful counter-terrorism efforts but an understanding of the systemic context in which seaports exist has to a basis from whence policy and strategy is developed. The terminal operator is not an individual cog in a wheel. Rather, the individual terminal operator is a system within a system within a system. The real challenge is that from an economic logic perspective, the evolution of the modern international trading system and its subset of intermodal transportation has developed with efficiency and the ability to conduct "just in time delivery" throughout the world. However, retrofitting that system with security integrated logics is the next challenge. After all, if the seaport truly is a system of systems, it is not sufficient that one country has resilient seaports. The nature of the supply chain is such that each link

becomes essential to the overall success. Thus, each link would have to be resilient for the entire system to truly be considered resilient at an individual level as well.

4.5 Implications for the Public Sector: Managing Hybridity

From a public policy perspective, an important conclusion derived from my analysis is that implementing security logics within the complex, hybrid organizations that define critical infrastructure management is a primary issue for the design and implementation of new laws and policies. Long before the terror event on 9/11, the Coast Guard was a trusted agent within the seaport community. Despite its multi-function nature as a regulatory, law enforcement, environmental, security and safety organization, the Coast Guard also carried a long-time reputation as a competent – and perhaps even necessary – presence in the maritime community. As a public agency, the Coast Guard had fostered relationships with the private sector for years and encouraged ongoing dialogue with the private sector. Thus, in terms of managing the public-private interface associated with introduction of security logics into the sphere of dominant economic logics, the trusted public agent had pre-existing relationships as well as working knowledge of the myriad issues already facing the private sector seaport community.

Decades of dialogue and collaboration meant that introduction of new security logics was done not so much as a forced imperative but rather as a true public-private partnership in every sense of the term. This collaborative approach likely eased the tensions normally associated with institutional change as private sector entities resigned themselves to the eventuality of institutional changes after 9/11.

Perhaps the most important part of the management of the public-private partnerships is learning to manage outcomes that truly bridge economic and security logics. Part of managing those outcomes is also managing the perceptions and expectations (and thus building trust) among the partners. I frequently heard from private sector interviewees about their distrust toward the intentions and competencies of public sector actors. For instance, one respondent reflected on the lessons learned from his experience in both the public and private sectors by relating his opinion of the way government typically frames the problem of security in private sector contexts, remarking that public officials often cynically view partnerships as "a new way to say the private sector is going to pay for something because we don't have the money; and that will never work, there has to be a business case to drive it. (Doan, personal communication, March 4, 2016).

In contrast, Mr. Doan seems to argue that policy makers need to recognize the long-term value to integrating security logic into the economic logic paradigm. In his perspective, a security program has "to be real and it can't be fake because if you are going to ask the private sector to come up with money and come up with new processes or whatever – they are going to do that only if they know that there is a business case that can drive it and way, way too often the government doesn't think about that, they are only thinking about what they need." (Doan, personal communication, March 4, 2016). Instead of viewing security as simply a resource sink[9] for both public and private actors,

[9] A 2011 study considered the cost-effectiveness of U.S. security expenditures including the aforementioned terrorism insurance. "To be considered cost-effective, American homeland security expenditures would have had each year to have foiled up to 1,667 attacks roughly like the one intended on Times Square in 2010 – more than four a day" (Mueller & Stewart, 2011). This study contained two tables, provided at the end of this chapter. The first of the two tables, Table 4.1, is the total homeland security

he instead seems to suggest that the construction of hybridized logics blending the security and the economic logics can lead to effective and sustainable security programs over the long term.

One of the unique aspects of this study is considering the long-term effects of new actors, governance issues and changing the rules by which existing (and new) actors play. However, incumbent upon the actors who are involved with creating security-logic driven policy is the underlying mandate that these actors should understand the unintended consequences and cascading effects of security-logic driven institutional changes.

4.6 CONCLUSION

Quis custodiet ipsos custodes?
[Who watches the watchmen?]
-Juvenal

Through this research study, the presence of an ideal type security logic has been identified. Distinctions have been made between security actors and security logics. The language and rhetoric after 9/11 raised the salience of this logic in both political and economic discourse. In the immediate aftermath of a punctuated terror attack, the security logic gains primacy. Yet, over time, as both public and private sectors return to the "new normal," the salience of the economic logic beings to emerge and we see private actors beginning to think about security logics over time. This connection between logics and actors occurs in a microcosm for an industry like that represented by maritime

expenditures by the U.S. Government between 2002 and 2011. The second table, Table 4.2, is better known as the "Trillion Dollar Table" as it shows all security expenditures during the same time period.

seaports. A finite number of actors must contend with the effects of multiple logics interacting.

In practice, we looked at institutional change not as the replacement of one type of change with another – or one type of logic with another – but instead as a blending activity of negotiation and change. What emerges from this blending is a hybridized form that helps ensure sustainability of the security programs and actual enhancements on security. Under certain conditions, it is possible that security logic as an independent logic might effectively lead to sustainable solutions as well. Nonetheless, any future research along this line that looks at the role of security as an independent logic needs to see it as embedded in the institutional structures that change and are contested over time.

Further, this study suggests that understanding the ramifications of blending logics and more importantly, hybridizing security and economic logics holds the potential to contribute to long term and sustainable implementation of security measures. A resilient seaport is the operationalization of hybridized logics. The very concept that both security and market logics can interact and emerge as a hybridized logic is the same idea that drives resiliency. Resiliency is not simply gates, guns and guards. It is the integration of security and sound business practices to create a system that is capable of returning to an operational status as quickly as possible after an event. While it is doubtful that resiliency has been described in this theoretical vernacular, the very concept of creating a system that hybridizes the various strategies into a new approach is exactly right. That is, if resiliency is the future of maritime security, then hybridization of logics is the key to effectively interpreting and perhaps anticipating the changing boundary conditions of logics and considering the form that an ideal hybridization would take

resulting in new governance forms and sustainable MNC strategies and public policies for the future.

While this study considers a specific problem set associated with multiple institutional logics, post-9/11 and critical infrastructure, there exists a whole host of issues that are related and as yet, unresearched. I have learned that a researcher must make judgment calls as to what is within the boundary conditions of the study and what lies outside. There is a virtual Greenfield of research opportunities in the future for this nascent branch of institutional logics and international business. Unfortunately, issues of terrorism, particularly in the context of anti-globalism, are infinitely complex and will not be resolved in one dissertation or over the course of the six years it took to earn this degree. Terrorism as it relates to MNCs, international business as a field, and society as a whole is a generational challenge.

Part of this generational challenge is to reconsider how to successfully implement public-private partnerships and the incentive for making the entire international system a viable public-private partnership in terms of counter-terrorism:

> If we take the perspective that what we are trying to secure is the continuity of the operation of the MTS [Marine Transportation System] in the face of people who are trying to exploit or target that system as a means of warfare, than what we have is a clear bridge for public and private cooperation. You can't make profit if it is not operating. Therefore, if we are talking about risk that could affect those operations in a potentially extended period of time – a time that could even threaten the viability of them as commercial enterprises - that should get their interest. That's a core responsibility they have as corporate officers connected within that enterprise (Interview 44, 2016).

Building on the idea that the seaport is part of the greater system, this interviewee is getting at the very heart of what motivates the private sector side of the public-private

partnership. The recipe for incentivizing private sector firms to form strong public partnerships is the knowledge that doing so achieves some greater public good – which may or may not be a motivator – but also that the survivability of the firm itself is at stake. Obviously, maintaining shareholder value also requires that the firm be in a condition to operate. Failure to provide the necessary security is not an option, then, for corporate officers within the firm. This again reinforces my research stating that the hybridization of logics can help transform the institution in a manner that leads to both effective and sustainable security programs. However, it is not enough to simply have a security program imposed as a cost center that eventually must compete with other budget priorities from a potential position of weakness as the original event which prompted the need for the security program recedes over time. Security is far more sustainable and palatable when the security is incorporated into the day-to-day operation – not superimposed but actually built into the system, similar to the hybridized logics that do not simply replace something else but go beyond blending to develop a new approach. Part of this approach also marries the strengths of the public and private sectors, when appropriate, to form public-private partnerships resulting in collaborative approaches to identifying and combating threats.

Given this discussion, it seems evident that there is much more research to be done in the field of international business and how it relates to terrorism and security in general. The work ahead is available at all levels of inquiry from the individual firm to the industry to the global levels. I think it will prove to be a rich research stream for at least the next 25 years. Not only is it rich in content, it is likely to prove beneficial to millions who suffer under the threat of terrorism and radical violence.

Thus will I close this chapter with something poignant that one of my interviewees said to me while discussing which side of the balance sheet to place funds spent on security:

> Security is an expense in the sense that tightening security makes it harder for the bad guys and businesses pass on that cost to their customers…. But it is also an investment as we are hardening our vulnerabilities. So it is probably a little of both…
>
> What is it that we want? As a society, what is it that we want? We want our flights to be more secure but we don't want to take our shoes off… we want to be safe in movie theater but you don't want to see a policeman at the ticket booth…What is it that the public wants? (Interview 11, 2016).

Understanding the effect of terrorism on the global business environment is a key component if advances in trade and open borders brought about by globalism are to continue unabated. As it is, isolated terror incidents around the world are giving rise to xenophobia, restrictions on labor flow, civil unrest and in the case of Europe, it might also serve as one of many factors attempting to drive the large trading bloc apart. If we are to answer the interviewee's question above about what the public wants, we must seek solutions through a better understanding of the long term consequences of transnational terrorist events in shaping public-private boundaries.

TABLE 4.1: TOTAL AND ENHANCED HOMELAND SECURITY EXPENDITURES BY THE U.S. GOVERNMENT, 2002 TO 2011, IN MILLIONS OF DOLLARS

Table 1.1 TOTAL AND ENHANCED HOMELAND SECURITY EXPENDITURES BY THE U.S. GOVERNMENT, 2002 TO 2011, IN MILLIONS OF DOLLARS

Year	Department							Total in current dollars	Total in 2010 dollars	Enhanced expenditure since 2001 in 2010 dollars
	Homeland Security[6]	Defense[8]	Health and Human Services[7]	Justice[8]	Energy[9]	State[10]	Others[11]			
2001	-	-	-	-	-	-	-	20,100[1]	24,723	-
2002	-	-	-	-	-	-	-	32,000[2]	38,720	13,997
2003	23,063	8,442	4,144	2,349	1,408	634	2,407	42,447[3]	50,087	25,364
2004	22,923	7,024[12]	4,062	2,180	1,364	696	2,585	40,834[3]	46,959	22,236
2005	24,549	17,188	4,229	2,767	1,562	824	3,264	54,383[3]	60,909	36,186
2006	26,571	17,510	4,352	3,026	1,702	1,108	2,849	57,118[3]	61,687	36,964
2007	29,554	16,538	4,327	3,517	1,719	1,242	2,936	59,833[3]	62,825	38,102
2008	32,740	17,374	4,301	3,523	1,829	1,962	3,194	64,923[3]	65,572	40,849
2009	38,988	19,483	4,677	3,715	1,939	1,809	3,385	73,996[3]	75,476	50,753
2010	36,081	19,041	4,804	4,107	2,018	1,767	3,252	71,070[3]	71,070	46,347
2011	37,066	19,103	5,428	4,285	2,023	2,258	2,349	72,512[4]	72,512	47,789
Total in 2010 dollars	286,781	149,130	42,888	31,078	16,489	12,824	27,908	567,098	605,818	358,588

Notes for this table begin on p. 196.

Source: Mueller & Stewart, 2011.

TABLE 4.2: THE TRILLION DOLLAR TABLE: ENHANCED COSTS OF HOMELAND SECURITY SINCE 9/11, IN BILLIONS OF 2010 DOLLARS

Table I.2 THE TRILLION DOLLAR TABLE: ENHANCED COSTS OF HOMELAND SECURITY SINCE 9/11, IN BILLIONS OF 2010 DOLLARS

	2009	2002–2011
Enhanced Direct Expenditures		
Federal "homeland security" expenditures from table I.1	50	360
Federal intelligence expenditures[13]	15	110
Local and state expenditures[14]	10	110
Private-sector spending[15]	10	110
Total[16]	**85**	**690**
Opportunity Costs		
Terrorism risk insurance premiums[17]	4	40
Passenger delays caused by airport screening[18]	10	100
Increase in short-haul traffic fatalities for people avoiding airport delays[19]	3	32
Deadweight losses and losses in consumer welfare[20]	30	245
Total	**47**	**417**
TOTAL	**132**	**1107**

Relevant spending elements not included in the table

Terror-related wars in Iraq and Afghanistan[21]

Costs of crime facilitated by focus of police and FBI on, or preoccupation with, terrorism

Costs resulting from Hurricane Katrina that might have been mitigated if DHS had not been so preoccupied by terrorism

Additional post office expenditures to deal with the effects of 9/11 and the anthrax letters[22]

Effects on tourism, property and stock market values, business location decisions, and so on, though deadweight losses might capture some of these

Source: Mueller & Stewart, 2011.

REFERENCES

154 Cong. Rec. S13, 17698 (daily ed. July 31, 2008) (statement by Sen. Coleman).

AAPA: Glossary of Maritime Terms. (n.d.). American Association of Port Authorities. Retrieved on 2016, July 10 from http://www.patnt.com/content/Glossary_of_Maritime_Terms.pdf.

Abadie, A. & Dermisi, S. (2008, September). Is terrorism eroding agglomeration economies on central business districts? Lessons from the office real estate market in downtown Chicago. *Journal of Urban Economics* 64(2), 451-463.

Abugumiza, K. (2015, July 28). Palestinian Seaport Authority [PowerPoint slides]. Retrieved from http://www.euromedtransport.org/image.php?id=1483.

Ackerman, E. & Rogers, P. (2001, October 18). National ID card idea attracting highest-level support. *San Jose Mercury News*. Retrieved from http://rense.com/general15/nationalIDcard.htm.

The American Waterways Operators, 2008 Annual Report. Retrieved from http://www.americanwaterways.com.

The American Waterways Operators, 2009 Annual Report. Retrieved from http://www.americanwaterways.com.

Arnon, A., Spivak, A., & Sussman, O. (2003, August). Incomplete Contracts, the Port of Gaza, and the Case for Economic Sovereignty. Retrieved from http://www.bgu.ac.il/~arnona/INCOMPLETE_CONTRACTS_PORT_OF_GAZA_AND_SOVEREIGNTY2004.pdf.

Associated Press. (2006, February 2). Coast Guard was unable to analyze port risks. NBC News.com. Retrieved from http://www.nbcnews.com/id/11596240.

Associated Press. (2008, May 27). Investigators find gaps in port security program. *USA Today Online*. Retrieved from http://usatoday30.usatoday.com/news/washington/2008-05-27-311029385_x.htm.

Aviation Transportation Security Act. Pub.L. 107–71 November 19, 2001.

AWO Testifies on TWIC at Coast Guard Subcommittee. (2007, July 20). *American Waterways Operators Letter Online* 64(13), 1. Retrieved from http://www.americanwaterways.com/sites/default/files/legacy/press-room/newsletter/07-20-07non.pdf.

Baker, D. (2014, September 11). FBI: attack on PG&E South Bay Substation wasn't terrorism. *SFGate*. Retrieved from http://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php.

Battilana, J. & Lee, M. (2014). Advancing research on hybrid organizing: Insights from the study of social enterprises. *The Academy of Management Annals* 8(1): 397-441.
Beisecker, R. (2006, March 1). Nuclear Threat Initiative. *DP World and U.S. Port Security*. Retrieved from http://nti.org/4269A.

Berman, J. (2015, November 11). U.S. Rep Hahn renews call for 100 percent cargo container scanning. *Logistics Management*. Retrieved from http://www.logisticsmgmt.com/article/u.s._rep._hahn_renews_call_for_100_percent_cargo_container_scanning.

bin Laden, O. (2004, November 1). Speech [Transcript, videotape sent to *Aljazeera*]. http://www.aljazeera.com/archive/2004/11/200849163336457223.html.

Birkinshaw, J., Brannen, M., & Tung, R. (2011). From a distance and generalizable to up close and grounded: Reclaiming a place for qualitative methods in international business research. *Journal of International Business Studies* 42(5), 573-581.

Black, C. (2005, January). TSA starts TWIC tests. *Biometric Technology Today*. 13(1).

Blalock, G., Kadiyali, V. & Simon, D. (2005, February 23). The impact of post 9/11 airport security measures on the demand for air travel. Retrieved from http://blalock.dyson.cornell.edu/wp/airport_security_022305.pdf.

Bliss, J. (2012, August 13). U.S. backs off all-cargo scanning goal with inspections at 4%. *Bloomberg Online*. Retrieved from http://www.bloomberg.com/news/articles/2012-08-13/u-s-backs-off-all-cargo-scanning-goal-with-inspections-at-4.

Blustein, P., & Pincus, W. (2006, February 24). Port problems said to dwarf new fears. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/02/23/AR2006022302303.html.

Bondareff, J. & Scontras, K. (2012, December). Strategic Seaports. *Maritime Reporter and Engineering* News, 16.

Bonney, J. (2006, July 19). Eller attorney says DP World issue not settled. *Journal of Commerce Online*. Retrieved from http://www.joc.com/maritime-news/eller-attorney-says-dp-world-issue-not-settled_20060619.html.

Brinkman, Peter. "Port opening cargo terminal - no further review required." The Orlando Sentinel. Jun 12, 2015.

Brundage, D. (2011, May 4). Q&A: U.S. port security before and after 9/11, Interview with Peter Tirschwell [Podcast and transcript]. *Journal of Commerce*. Retrieved from http://www.joc.com/content/qa-us-port-security-and-after-911.

Burgelman, R. (2011). Bridging history and reductionism: A key role for longitudinal qualitative research. *Journal of International Business Studies*, 42(5), 591-601.

Busch, N. & Givens, A. (2012, October). Public-private partnerships in homeland security: opportunities and challenges. *Homeland Security Affairs* 8, Article 18. Retrieved from https://www.hsaj.org/articles/233.

Busch, N. & Givens, A. (2014). The Business of Counterterrorism, Public-Private Partnerships in Homeland Security. New York, NY: Peter Lang Publishing, Inc.

Bush, President G.W. (2001, September 20). Address to a Joint Session of Congress and the American People given at the U.S. Capitol [Transcript]. Retrieved from https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html.

Carafano, J. and Zuckerman, J. (2012, February 12). Maritime cargo scanning folly: bad for the economy, wrong for security. The Heritage Foundation. Retrieved from http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate.

Central Intelligence Agency, National Strategy for Combating Terrorism. (2003) Retrieved from https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

Chambers, M. (2010, October). U.S. Department of Homeland Security. Atlantic coast U.S. seaports. Retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/bts_fact_sheets/october_2010/html/entire.html.

Chen, A. & Siems, T. (2004, June). The effects of terrorism on global capital markets. *European Journal of Political Economy*. 20(2), 249-366.

Clarke, R., Downing, W., Rice, C. & Ridge, T. (2001, October 11). New anti-terrorism officials announcement [Press briefing]. Retrieved from http://www.c-span.org/video/?166573-1/new-antiterrorism-officials-announcement.

Computer Security Act of 1987. (1988, January 8). Public Law No. 100-235 (H.R. 145).

Connors, B. (2010, June 18). Preparing for PS-Prep – voluntary private sector preparedness certification. *Security Debrief Blog*. Retrieved from http://securitydebrief.com/2010/06/18/preparing-for-ps-prep-voluntary-private-sector-preparedness-certification/.

Cooper, R. (2009, November 3). PS Prep – does anyone care? *Security Debrief blog*. Retrieved from http://securitydebrief.com/2009/11/03/private-sector-prep-does-anybody-care/.

Critical Infrastructure Protection. (1996, July). Exec. Order No. 13010, 61 Fed. Reg. 37347.

Critical Infrastructures Protection Act of 2001, 42 U.S. Code § 5195c (2006).

Criticism of Port Security Grant Program 'Misses the Mark'. (2005, February 9). MarineLink.com. Retrieved from http://www.marinelink.com/news/article/criticism-of-port-security-grant-program-misses/316882.aspx.

Cronin, Audrey. (2002/2, Winter). Behind the curve: globalization and international terrorism. *International Security* 27(3), 30–58.

Customs brokers are critical to a successful international supply chain (2014, May 9). International Trade Magazine. Retrieved from http://www.intrademagazine.com/customs-brokers-are-critical-to-a-successful-international-supply-chain-2/.

Czinkota, M., Knight, G., & Liesch, P. (2004). Terrorism and international business: conceptual foundations. In G. Suder, (Ed.), *Terrorism and the International Business Environment.* The Security Business Nexus: 43–57. Edward Elgar Publishing.

Czinkota, M., Knight, G., Liesch, P., & Steen, J. (2010, June). Terrorism and International Business: A Research Agenda. *Journal of International Business Studies*. 41(5), 826-843.

Dawes, S. (1996), Interagency information sharing: expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*. 377–394. doi: 10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F.

DHL United States of America. (n.d.). International Trade Advice to Help Grow Your Business Globally. Retrieved on July 9, 2016 from http://www.dhl-usa.com/en/express/small_business_solutions/business_across_borders/trading_internationally.html.

DiMaggio, P. & Powell, W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review,* 48(2). 147–160.

DiMaggio, P. & Powell, W. (Eds.). (1991). The new institutionalism in organizational analysis. Chicago, IL: University of Chicago Press.

Doan, D. (2016, March 4). Personal communication [Interview].

Dooley, Cal. (2012, July 18). Letter to the Honorable John Mica. American Chemistry Council. Retrieved from https://www.americanchemistry.com/Policy/Rail-Transportation/Letter-to-Chairman-Mica-and-Ranking-Member-Rahall.pdf.

Doty, D. & Glick, W. (1994). Typologies as a unique form of theory building: toward improved understanding and modeling. *Academy Of Management Review*, 19(2), 230-251. doi:10.5465/AMR.1994.9410210748.

DP World: Anatomy of a Crisis. (2006, March 1). *Material Handling and Logistics*. Retrieved from http://mhlnews.com/global-supply-chain/dp-world-anatomy-crisis.

DuPont, M. (2016, February 22). Personal communication [Interview].

Enders, W., Sandler, T. & Gaibulloev, K. (2011, May). Domestic versus transnational terrorism: data, decomposition, and dynamics. *Journal of Peace Research* 48, 319-337.

Facility Security, U.S. Coast Guard, 33 C.F.R. § 60515 (2003, November 22).

Federal Emergency Management Agency. (n.d.). About PS-PrepTM. Retrieved 2016, July 16 from https://www.fema.gov/about-ps-preptm.

Federal Maritime Commission. (n.d.). About us. Retrieved 2015, September 15 from http://www.fmc.gov/about/about_fmc.aspx.

Federal Maritime Commission. (n.d.). Marine terminal operators. Retrieved on 2016, June 22 from http://www.fmc.gov/resources/marine_terminal_operators.aspx.

Fernandez, M. (2009, June 26). The 100% container scanning legislation: an analysis of waiting lines and economic costs [Unpublished thesis]. Retrieved from http://www.ecorys.com/sites/default/files/files/Pillar%206%20CD17500%20-%20100%20container%20scanning.pdf.

Finkin, E. (2006, February 23). Update on DP World purchase of P&O terminal operations [Letter]. Retrieved from http://www.portmod.org/MEMBERSONLY/DP%20World%20Update.pdf

Florida Department of Transportation, Seaport System. (n.d.). Retrieved on 2015 October 4 from http://www.dot.state.fl.us/seaport/seamap.shtm.

Florida Department of Transportation. (n.d.). Seaport system: Florida. Retrieved on 2015 October 5 from http://www.dot.state.fl.us/seaport/seamap.shtm.

Florida Ports Council. (2015). Competitive, Committed, Connected: State of Florida's Seaports, 2015. Retrieved from http://static.flaports.org/State-of-Florida-Ports-2014-15-Final-Revised-3252015web.pdf.

Florida Ports Council. (n.d.). Florida Ports Council: About Us. Retrieved 2015, March 26 from http://flaports.org/about/florida-ports-council/.

Flynn, S. (2006). The continued vulnerability of the global maritime transportation system [Written testimony, Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, United States House of Representatives].

Flynn, S. (2012, July 11). The new homeland security imperative: The case for building greater societal and infrastructure resilience [Written Testimony, Committee on Homeland Security and Government Affairs, U.S. Senate].

Form LM-2 Labor Organization Annual Report for 2014. Longshore & Warehouse Union AFL-CIO National HQ. March 26, 2015.

Form LM-2 Labor Organization Annual Report for 2015. Longshoremen's Association AFL-CIO. U.S. Department of Labor. March 31, 2015. Web. <https://olms.dol-esa.gov/query/orgReport.do>>

Frey, B. (2009) How can business cope with terrorism? *Journal of Policy Modeling* 31, 779-787.

Friedland, R. & Alford, R. R. (1987). Bringing Society Back In: Symbols, Practices, and Institutional Contradictions. In Lash, S. & Whimster, S. (Eds.), *Max Weber, Rationality and Modernity* (pp. 232-263). London: Allen & Unwin.

Friedland, R. & Alford, R. (1991). Bringing society back in: symbols, practices and institutional contradictions. *The New Institutionalism in Organizational Analysis.* W. Powell & P. DiMaggio (Eds.). Chicago, IL: University Of Chicago Press.

Friedman, M. & Sherman, T. (2013, June 4). Frank Lautenberg leaves a legacy of fighting for N.J. and beyond. *The Star Ledger* via NJ.com. Retrieved from http://www.nj.com/politics/index.ssf/2013/06/frank_lautenberg_dead_at_89_le.html.

Frittelli, J. (2005, May 27). Port and Maritime Security: Background and Issues for Congress." CRS Report for Congress. Washington, DC May 27, 2005.

Gaddis, J. L. (2002). *The landscape of history: how historians map the past*. New York, NY: Oxford University Press.

Garud, R., Jain, S., & Kumaraswamy, A. (2002). Institutional entrepreneurship in the sponsorship of common technological standards: The case of Sun Microsystems and Java. *Academy of Management Journal*, 45(1): 196–214.

Ghobari, M. & Sleiman, M. (2013, September 19). Blackout hits large parts of Yemen after attack on power lines. *Reuters*. Retrieved from http://www.reuters.com.

Gidick, K. (2015, October 5). Measuring the Charleston storm by the Waffle House Index: smothered, covered, and flooded. *Charleston City Paper*, 5 Oct 2015. Retrieved from http://www.charlestoncitypaper.com/Eat/archives/2015/10/05/measuring-the-charleston-storm-by-the-waffle-house-index.

Gilmour, T. (2006, March 2). Statement on the national security review of the DP World transaction before the Armed Services Committee, U.S. House of Representatives.

Glaser, B. (1992). *Basics of grounded theory analysis: emergence vs. forcing*. Mill Valley, CA: Sociology Press.

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research* (Reprinted 2006 ed.). London (U.K.): Aldine Transaction.

Glynn, M.A. and Lounsbury, M. (2005). From the critics' corner: logic blending, discursive change and authenticity in a cultural production system. *Journal of Management Studies*, 42, 1031-1055.

Government Accountability Office. (2003). Progress made in implementing maritime transportation security act, but concerns remain. (GAO Publication No. 03-1155T). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2004). Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. (GAO Publication No. 05-106). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2006). Transportation security: DHS should address key challenges before implementing the Transportation Worker Identification Credential Program. (GAO Publication No. 06-982). Washington, DC: U.S. Printing Office.

Government Accountability Office. (2007). Port risk management: additional federal guidance would aid ports in disaster planning and recovery. (GAO Publication No. 07-412). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2008). Transportation Worker Identification Credential: a status update [Testimony before the House Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security]. (GAO Publication No. 08-1151T). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2009). Progress made in enrolling workers and activating credentials but evaluation plan needed to help inform the implementation of readers. (GAO Publication No. 10-43). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2011). Internal control weaknesses need to be corrected to help achieve security objectives. (GAO Publication No. 11-657). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2011). Port security grant program: risk model, grant management, and effectiveness measures could be strengthened. (GAO Publication No. 12-47). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2013). Defense logistics: the Department of Defense's report on strategic seaports addressed all congressional directed elements. (GAO Publication No. 13-511R). Washington, DC: U.S. Government Printing Office. Retrieved from http://www.gao.gov/assets/660/654578.pdf.

Graham, Bob. Congressional Record-Senate. Washington, D.C. Jul 27, 2000. In Congressional Record, V. 146, Pt. 12, July 27, 2000 to September 13 2000. (P. 16787).

Groat, L. & Wang, D. (2002) *Architectural Research Methods*. New York, NY: John Wiley & Sons, Inc.

Greenbaum, R., Dugan, L. & LaFree, G. (2007, May). The impact of terrorism on Italian employment and business activity. *Urban Studies*, 44(5/6), 1093-1108.

H.R. Res. 344, 109th Cong. 1 (2005). Expressing the sense of the House of Representatives that a Chinese state-owned energy company exercising control of critical United States energy infrastructure and energy production capacity could take action that would threaten to impair the national security of the United States. Retrieved from https://www.congress.gov/bill/109th-congress/house-resolution/344/text#.

Hamilton, A. (1791, June 4). Instructions to the commanding officers of the revenue cutters [Letter]. Retrieved from https://www.uscg.mil/history/faqs/hamiltonletter.pdf.

Hargrave, T. J., & Van De Ven, A. H.. (2006). A Collective Action Model of Institutional Innovation. *The Academy of Management Review*, *31*(4), 864–888. Retrieved from http://www.jstor.org/stable/20159256

Harrald, J. (2010, March). New paradigms for private sector preparedness [Testimony to the Homeland Security and Governmental Affairs Committee, Ad Hoc Sub-committee on State, Local and Private Sector Preparedness and Integration].

Haveman, J., Shatz, H. & Vilchis, E. (2006). The government response: U.S. port security programs in protecting the nation's seaports: balancing security and cost. Haveman, J. & Shatz, H. (Eds.). San Francisco, CA: Public Policy Institute of California.

Hecker, J. (2002, August 5). Port security: nation faces formidable challenges in making new initiatives successful [Testimony before the Subcommittee on National Security, Veterans Affairs and International Relations, House Committee on Government Reform].

Henisz, W. & Zelner, B. (2003, December). The strategic organization of political risks and opportunities. *Strategic Organization* 1(4), 451-460.

The Heritage Foundation. (n.d.). The U.S. and Int'l Response to 911. Retrieved on 2016, July 9 from http://www.heritage.org/research/projects/enemy-detention/response-to-911.

Hollings, Ernest. Congressional Record-Senate. Washington, D.C. Jul 27, 2000. In Congressional Record, V. 146, Pt. 12, July 27, 2000 to September 13 2000. (P. 16785).

Holm, P. (1995). The Dynamics of Institutionalization: Transformation Processes in Norwegian Fisheries. *Administrative Science Quarterly*, 40(3), 398-422.

Hopkins, D. (2009, February). New focus on private-sector preparedness standards. *Domestic Preparedness Journal* 5(2). Retrieved from http://www.domesticpreparedness.com/pub/docs/DPJournalFeb09.pdf.

House Report on Energy and Water Development Appropriations Bill. H. Rep. No. 109-474 (2007).

Hunter, Duncan. "Is it racist to ban Arab companies from operating U.S. ports." Written for CQ Researcher, April 2006.

Identity Security and Modernization of the Merchant Mariner Credential Statute; U.S. Department of Homeland Security Notice of Public Meeting and Request for Comments. 70 Fed. Reg. 96. ((2005, May 6). Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2005-05-19/pdf/05-9936.pdf.

Iftikhar, Arsalam T. "Is it racist to ban Arab companies from operating U.S. ports." Written for CQ Researcher, April 2006.

ILWU wants to scrap TWIC. (2012, July 3). *World Cargo News Online*. Retrieved from http://www.worldcargonews.com/htm/w20120703.860269.htm.

Implementing Recommendations of the 9/11 Commission Act of 2007, PUBLIC LAW 110–53 (2007, August 3).

Information sharing efforts are improving [Testimony before the Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform, House of Representatives]. 109th Cong. 2 (2006, July 10). Retrieved from http://www.gao.gov/new.items/d06933t.pdf.

Institute for the Analysis of Global Security. (n.d.) How much did the September 11 terrorist attack cost America? Retrieved on 2016, April 13 from http://www.iags.org/costof911.html.

Interagency Commission on Crime and Security in U.S. Seaports. (2000). Report of the Interagency Commission on Crime and Security in U.S. Seaports : Abstract.

International Brotherhood of Boilermakers. (n.d.). About the Boilermakers. Retrieved on 2015, October 10 from https://www.boilermakers.org/about.

International Brotherhood of Teamsters, Safety and Health Department. (n.d.). Transportation Worker Identification Credential (TWIC) program. Retrieved from https://teamster.org/sites/teamster.org/files/TWIC.pdf.

Investing in tourism: analyzing the economic impact of expanding Florida tourism. (2013). *Florida Tax Watch*. Retrieved from http://floridataxwatch.org/resources/pdf/2013TourismFINAL.pdf.

ISO 22301:2012(E). Societal security – business continuity management systems – requirements. (2012, May 5). International Organization for Standardization. Geneva, Switzerland.

Jackson, M. (2006, March 1). Testimony of Deputy Secretary Michael Jackson before the Committee on Financial Services, Subcommittee on Domestic and International Monetary Policy, Trade and Technology.

Joint Resolution to Authorize the Use of United States Armed Forces, Pub. L. 107-40, 115 Stat. 224 (2001).

Kahaner, L. (2008, June 1). One card united. *Fleet Owner*. Retrieved from http://fleetowner.com/information_technology/feature/one_card_united_0601.

Kaplan, E. (2006, February 21). The UAE purchase of American port facilties. Council on Foreign Relations. Retrieved from http://www.cfr.org/border-and-port-security/uae-purchase-american-port-facilities/p9918.

Kenny, M., & Fourie, R. (2014). Tracing the history of grounded theory methodology: From formation to fragmentation. *The Qualitative Report*, 19(52), 1.

Kolar, P. & Puckett, S. (2011, September 28-30). Role of port authorities in Australia, Canada and the European Union [Paper for Australasian Transport Research Forum 2011 Proceedings]. Retrieved from http://atrf.info/papers/2011/2011_kolar_puckett.pdf.

Krepp, D. (2012, December 10). How do you fix a broken TWIC? JOC.com. Retrieved from https://www.joc.com/regulation-policy/transportation-regulations/united-states/how-do-you-fix-broken-twic_20121210.html.

Kunreuther, H. (2002, April). The role of insurance in managing extreme events: implications for terrorism coverage [Working paper, Wharton Financial Institutions Center] . Retrieved from http://fic.wharton.upenn.edu/fic/papers/02/0207.pdf.

Langen, P.W. de. (2002). Clustering and performance: the case of maritime clustering in The Netherlands. *Maritime Policy & Management*. 29(3).

Larson, A. & Marchik, D. (2006, July). Foreign investment and national security: getting the balance right [CSR 18]. Council on Foreign Relations.

Lawless, J. (2012, June 28). Spoken testimony before the House Committee on Transportation and Infastructure. Washington, DC.

Li, L., Li, J., Qian G., and Qian, Z. (2008). Regional diversification and firm performance. *Journal of International Business Studies*. 39(2), 197-214.

Li, S., & Tallman, S. (2011). MNC strategies, exogenous shocks, and performance outcomes. S*trategic Management Journal* 32(10), 1119–1127. DOI: 10.1002/smj.918

Lipowicz, A. (2009, February 11). TWIC program has woes with PIN resets. FCW.com. Retrieved from https://fcw.com/articles/2009/02/11/twic.aspx.

Magnet, A. (2006, February 14). Schumer calls for probe of Arab port deal. *New York Sun*. Retrieved from http://www.nysun.com/new-york/schumer-calls-for-probe-of-arab-port-deal/27530/.

Maritime labor testifies at TWIC oversight hearing. (2007, July 20). *West Coast Sailors, Official Organ of the Sailors' Union of the Pacific*, 70(7). Retrieved from http://www.sailors.org/sites/default/files/newsletter/pdf/wcs-july2007.pdf.

Maritime Security: Area Maritime Security, U.S. Coast Guard, 33 C.F.R. Part 103 (2003, October).

The Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, § 102, 116 Stat. 2073 (2002).

Maslow, A.H. (1943). A theory of human motivation. *Psychologial Review* 50, 370-396. Retrieved from http://psychclassics.yorku.ca/Maslow/motivation.htm.

McAdam, D. (1982). Political process and the development of black insurgency, 1930–1970. Chicago, IL: University of Chicago Press.

Meyer, J. R., & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology,* 83(2), 340–363. Retrieved from http://www.jstor.org/stable/2778293.

Morrill, C. (2016). Institutional change through interstitial emergence: the growth of alternative dispute resolution in American law, 1965-1995 [Unpublished manuscript, University of Arizona, Tucson, AZ]. Retrieved from http://webuser.bus.umich.edu/organizations/smo/protected/resources/morrill.pdf.

Morris, C. & Frey, R.G. (Eds.). (1991). *Violence, Terrorism and Justice.* New York, NY: Cambridge University Press.

Moskowitz, L. (2008, September 17). Transportation Worker Identification Credential: a status update [Testimony before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism].

Moteff, J. (2012, August 23). Critical infrastructure resilience: the evolution of policy and programs and issues for Congress. Congressional Research Service, Washington, D.C. Retrieved from https://www.fas.org/sgp/crs/homesec/R42683.pdf.

Mueller, J. & Stewart, M. (2011). *Balancing the risks, benefits and costs of homeland security*. New York, NY: Oxford University Press.

Murphy, P. R., & Daley, J. M. (2001). Profiling international freight forwarders: an update. *International Journal of Physical Distribution & Logistics Management*, 31(3), 152.

Murray, F. (2010). The oncomouse that roared: hybrid exchange strategies as a source of distinction at the boundary of overlapping institutions. *The American Journal of Sociology*, 116(2), 341-388.

Napolitano, J. (2009, July 29). Remarks by Secretary Napolitano at the Council on Foreign Relations. Retrieved from https://www.dhs.gov/news/2009/07/29/secretary-napolitanos-remarks-council-foreign-relations.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission report*. Washington, DC: U.S. Government Printing Office.

National Maritime Security Advisory Committee TWIC Working Group Discussion Points. (2008, July 30). Retrieved from http://www.maritimedelriv.com/Port_Security/TSA/files/NMSAC_TWG_recommendations_amended.pdf.

National Research Council. (2011). Building Community Disaster Resilience Through Private-Public Collaboration. Washington, DC: National Academies Press.

National Strategy for Combating Terrorism. (2003, February). Retrieved from https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

Naval Air Station Jacksonville. (n.d.). Welcome to Naval Air Station Jacksonville, U.S. Navy. Retrieved on October 4, 2015 from http://www.cnic.navy.mil/regions/cnrse/installations/nas_jacksonville.html.

Nigam, A. and Ocasio, W. (2010). Event attention, environmental sensemaking, and change in institutional logics: An inductive analysis of the effects of public attention to Clinton's health care reform initiative. *Organization Science*, 21, 823-841.

North, D. (1991). Institutions. *The Journal of Economic Perspectives, 5*(1), 97-112. Retrieved from http://www.jstor.org/stable/1942704.

Office of Management and Budget. (Exp. 2018, March 31). Security plans for ports, vessels, facilities, and outer continental shelf facilities and other security-related requirements. (OMB Circular 1625-0077). Washington, DC.

Overby, P. (2006, March 8). Lobbyist's last minute bid set off ports controversy [Transcript of radio interview]. National Public Radio.

Pache, A.C. & Santos, F. (2010). When worlds collide: the internal dynamics of organizational responses to conflicting institutional demands. *Academy of Management Review*, 30(3), 455-476.

Pacific Maritime Association. (n.d.). Pacific Maritime Association: what we do. Retrieved on 2015 September 10 from http://www.pmanet.org/overview.

Perrow, C. (2006, April). The disaster after 9/11: the Department of Homeland Security and the intelligence reorganization. *Homeland Security Affairs* 2(3). Retrieved from https://www.hsaj.org/articles/174.

Port and Maritime Security Act of 2000 [Introduced]. 106th Cong. 2 (2000). Retrieved from https://www.congress.gov/bill/106th-congress/senate-bill/2965.

The Port Authority of New York and New Jersey. (n.d.). Overview of facilities and services. Retrieved on 2015 October 10 from http://www.panynj.gov/about/facilities-services.html.

The Port Authority of New York and New Jersey. (n.d.). PANYNJ: about us. Retrieved on 2015 October 10 from http://www.panynj.gov/about/.

The Port Authority of New York and New Jersey. (n.d.). PANYNJ: financial information. Retrieved on 2015 October 10 from http://corpinfo.panynj.gov/pages/financial-information/.

The Port Authority of New York and New Jersey. (n.d.). PANYNJ: governance. Retrieved on 2015 October 10 from http://corpinfo.panynj.gov/pages/governance/.

Port of Los Angeles. (2011, March). TWIC field test summary and key findings.

Powers, M. & Choi, S. (2012). Does transnational terrorism reduce foreign direct investment? Business-related versus non-business-related terrorism. *Journal of Peace Research* 49(3): 407-422.

Purdy J. & Gray, B. (2009). Conflicting logics, mechanisms of diffusion, and multilevel dynamics in emerging institutional fields. *Academy Of Management Journal* 52(2), 355-380.

Quinter, P. (2014, April 28). Customs brokers are critical to a successful international supply chain. Originally published in *International Trade Magazine*. Retrieved from http://www.lexology.com/library/detail.aspx?g=ee880285-8752-4067-9c9d-af7edcd4bf8c.

Rabkin, Norman J. "Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts." Testimony before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate. United States General Accounting Office: Washington, D.C. Mar 30, 2004. http://www.gao.gov/assets/120/110786.htm.

Rao, H., Monin, P., & Durand, R. (2003). Institutional Change in Toque Ville: Nouvelle Cuisine as an Identity Movement in French Gastronomy. *American Journal of Sociology,* 108(4), 795-843. doi:1. Retrieved from http://www.jstor.org/stable/10.1086/367917 doi:1

Reade C. (2009, August). Human resource management implications of terrorist threats to firms in the supply chain. *International Journal Of Physical Distribution & Logistics Management* 39(6), 469-485.

Reay, T. and Hinings, C.R. (2009). Managing the rivalry of competing institutional logics, *Organization Studies*, 30, 629-652.

Review of the Delays and Problems Associated with TSA's Transportation Worker Identification Credential: Hearing before the Committee on Transportation and Infrastructure, House of Representatives, 112th Cong. 2 (2012).

Rojas, Martin. (2008, February 26). Letter from the American Trucking Associations to the Transportation Security Administration. Retrieved from http://docplayer.net/14988256-American-trucking-associations-2200-mill-road-alexandria-va-22314-4677.html.

SAFE Port Act, Pub.L. 109–347. (2006).

Sandler, T. & Arce D. (2003, September). Terrorism and game theory. *Simulation and Gaming*. 34(3), 219-337.

Sandler, T. & Enders, W. (2008, February 11). Economic consequences of terrorism. In Philip Keefer & Norman Loayza (Eds.) *Terrorism, Economic Development, and Political Openness*. New York, NY: Cambridge University Press.

Scott, W. R. (2001). *Institutions and organization: ideas and interests,* 2nd Ed. Thousand Oaks, CA: SAGE Publications, Inc.

Sea port of embarkation (SPOE). (n.d.). Retrieved on July 9, 2016 from http://www.globalsecurity.org/military/facility/spoe.htm.

Seafarers International Union. (n.d.). Seafarers Homepage. Retrieved on 2015 October 6 from https://www.seafarers.org/index.asp.

Secretary Ridge announces steps in enhancing maritime security. (2003, October 23). MarineLink.com. Retrieved from http://www.marinelink.com/news/article/324444.aspx.

Security Council Resolution 1368. *Threats to international peace and security caused by terrorist acts*. (2001, September 12).

Security of terminal operations at U.S. ports: Opening statement before the Committee on Commerce, Science and Transportation, Senate, 109th Cong. 2 . (2006, February 28). (Testimony of Stevens, Ted). Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-109shrg71844/pdf/CHRG-109shrg71844.pdf.

Servidio, J.A. (2013, June 11). U.S. Coast Guard Commandant Instruction 16601.28A: Area Maritime Security Plan (AMSP) and Area Maritime Security (AMS) assessment development and maintenance process. Retrieved from https://www.uscg.mil/directives/ci/16000-16999/CI_16601_28A.pdf.

Sheffi, Y. (2002, May). Supply chain management under the threat of international terrorism [Working paper, MIT Engineering Systems Division]. ESD-WP-2003-01.27.

Shenon, P. (2003, April 29). Former domestic security aides switch to lobbying. *New York Times*. Retrieved from http://www.nytimes.com/2003/04/29/politics/29HOME.html?pagewanted=all.

Sherman, R. (2002). Seaport governance in the United States and Canada. & American Association of Port Authorities. Retrieved from http://www.aapa-ports.org.

Shipilov, A., Greve, H., and Rowley, T. (2010). When do interlocks matter? Institutional logics and the diffusion of multiple corporate governance practices. *Academy of Management Journal*, 53, 846-864.

Skelcher, C. and Smith, S.R. (2015). Theorizing hybridity: institutional logics, complex organizations, and actor identities: the case of nonprofits. Public Administration. 93(2), 433-448. DOI:10.1111/padm.12105.

South Carolina Port Authority. (2015). 2014 South Carolina port guide: South Carolina's seaports and infrastructure resource. Retrieved from https://issuu.com/scbiz/docs/2014_sc_port_guide.

South Carolina Ports Authority. (n.d.). Mission and leadership. Retrieved on 2015, September 10 from http://www.scspa.com/about/mission-and-leadership/

South Carolina Ports Authority. (n.d.). SC ports: board of directors. Retrieved on 2015, September 10 from http://www.port-of-charleston.com/About/boardofdirectors.asp.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures*
and techniques (1st ed.). Newbury Park, CA: Sage Publications.

Suder, G. & Czinkota, M. (2013). Terrorism studies in international business: increasing knowledge, reducing victimization. *AIB Insights,* 13(4). Retrieved from https://aib.msu.edu/publications/insights/volume/13/issue/4.

Suder, G. (Ed.). (2004). *Terrorism and the International Business Environment.* Northampton, MA: Edward Elgar Publishing.

Suder, G. (Ed.). (2006). *Corporate strategies under international terrorism and adversity*. Northampton, MA: Edward Elgar Publishing.

Teubner, R. (2002). Port Security Program Presentation, U.S. Coast Guard.

Thomson, J. (2007). DHS AWOL? Tough questions about homeland security have gone missing. *Rand Review Online*. Retrieved from http://www.rand.org/pubs/periodicals/rand-review/issues/spring2007/publisher.html.

Thornton, P. & Ocasio, W. (1999). Institutional logics and the historical contingency of power in organizations: executive succession in the higher education publishing industry, 1958-1990. *American Journal of Sociology*, 105(3), 801-843.

Thornton, P. & Ocasio, W. (2008). Institutional Logics. In R. Greenwood, C. Oliver, R. Suddaby, & K. Sahlin (Eds.), The Sage Handbook of Organizational Institutionalism (1-46). Los Angeles: Sage Publications.

Thornton, P. (2004). *Markets from Culture: Institutional Logics and Organizational Decisions in Higher Education Publishing*. Stanford, CA: Stanford University Press.

Thornton, P., Jones, C., & Kury, K. (2005). Institutional logics and institutional change in organizations: transformation in accounting, architecture and publishing. Transformation in Cultural Industries, Research in the Sociology of Organizations. 23, 125-170.

Thornton, P., Ocasio, W. & Lounsbury, M. (2012). The Institutional Logics Perspective: A New Approach to Culture, Structure and Process. New York, NY: Oxford University Press.

Tongzon, J. & Wu, W. (2005). Port privatization, efficiency and competitiveness: some empirical evidence from container ports (terminals). *Transportation Research Part A: Policy and Practice, Elsevier* 39(5), 405-424. Retrieved from https://ideas.repec.org/a/eee/transa/v39y2005i5p405-424.html#biblio-body.

Transport workers' ID card final rule released by gov't. (2007, January 19). *West Coast Sailors, Official Organ of the Sailors' Union of the Pacific*, 70(1). Retrieved from http://www.sailors.org/sites/default/files/newsletter/pdf/jan2007wcs.pdf.

Transportation Research Board of the National Academies, Panel on Transportation, Committee for Science and Technology for Countering Terrorism. (2002). Deterrence, Protection and Preparation: The New Transportation Security Imperative [Special report 270]. Retrieved from www.TRB.org.

Transportation Worker Identification Credential (TWIC) implementation in the maritime sector, hazardous materials endorsement for a commercial driver's license [Final rule;

Request for comments]. (2007, January 25). 71 FR 29396. Retrieved from https://federalregister.gov/a/07-19.

Tritak, John. (1999). National Information Systems Security Conference (NISSC) Panel Proposal. Washington, DC.

Trujillo, L. & Nombela, G. (1999, November). Privatization and regulation of the seaport industry [Working Paper, World Bank].

Tucci, D. (n.d.). The Coast Guard captain of the port then and now. Retrieved from http://www.uscg.mil/hq/cg5/cg544/docs/Captain%20of%20the%20Port.pdf.

TWIC Field Testing Underway. (2003, June).*Biometric Technology Today* 11(6).

TWIC Implementation – Phase One. (2007, January 25). Marinelink.com. Retrieved from http://www.marinelink.com/news/article/twic-implementation-phase-one/312544.aspx.

U. S. Department of Justice, Office of the Inspector General Audit Division. (2006, March). The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports. Audit Report 06-26.

U.S Department of Homeland Security, Transportation Security Administration. (n.d.). Surface transportation. Retrieved 2016 June 10 from https://www.tsa.gov/for-industry/surface-transportation.

U.S. Army Corps of Engineers, National Data Center. (2015). Ports and waterways facilities. Retrieved from http://www.navigationdatacenter.us/ports/ports.htm.

U.S. Army Corps of Engineers, National Data Center. (n.d.). Ports and Waterways Facilities. Retrieved on 2015, September 15 from http://www.navigationdatacenter.us/ports/ports.htm.

U.S. Coast Guard, Waterways Management Directorate. (2008, August). Harbor Safety Committee Desk Reference. Retrieved from http://www.uscg.mil/d17/sectoranchorage/prevention/wwmdocs/HSC%20Desk%20Ref%20of%20August%202008.pdf

U.S. Coast Guard. (2013, December 20). Area Maritime Security Committees Annual Report.

U.S. Department of Commerce, National Institute of Standards and Technology. (2001, February). NISSC 1977 – 2000. Retrieved from http://csrc.nist.gov/nissc/.

U.S. Department of Defense. (2008). National Defense Strategy. Retrieved from http://www.defense.gov/Portals/1/Documents/pubs/2008NationalDefenseStrategy.pdf.

U.S. Department of Health and Human Services, Food and Drug Administration Office of Criminal Investigations. (2012, July 25). $100 Million Customs Fraud Uncovered; President of San Diego Customs Brokers Association and Ten Others Charged in Scheme [Press release]. Retrieved from http://www.fda.gov/ICECI/CriminalInvestigations/ucm313527.htm.

U.S. Department of Homeland Security, Customs and Border Patrol. (n.d.). Cargo security and examinations. Retrieved 2015, October 10. Retrieved from http://www.cbp.gov/border-security/ports-entry/cargo-security.

U.S. Department of Homeland Security, Customs and Border Protection. (n.d.). CSI: Container Security Initiative. Retrieved on 2015, October 10 from http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief.

U.S. Department of Homeland Security, Customs and Border Protection. (n.d.). C-TPAT: Customs Trade Partnership Against Terrorism. Retrieved 2015, October 10 from http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism.

U.S. Department of Homeland Security, Homeland Security Advisory Council, Private Sector Information Sharing Task Force. (2015). Homeland Security Information Sharing Between Government and the Private Sector. Retrieved from https://www.dhs.gov/xlibrary/assets/HSAC_InfoSharing_FinalReport.pdf.

U.S. Department of Homeland Security, Homeland Security Advisory Council. (2006, January). Report of the Critical Infrastructure Task Force. Retrieved from https://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

U.S. Department of Homeland Security, Homeland Security Advisory Council. (2006, January 10). Critical Infrastructure Task Force, presentation to Homeland Security Advisory Council [PowerPoint slides]. Retrieved from https://www.dhs.gov/xlibrary/assets/CITF_Report_HSAC_Bl.pdf.

U.S. Department of Homeland Security, Maritime Administration. (2013). Factsheet: 2013 vessel calls in U.S. ports and terminals. http://www.marad.dot.gov/wp-content/uploads/pdf/DS_MARAD-2013-Vessel-Calls-Information-Sheet.pdf.

U.S. Department of Homeland Security, Office of Inspector General. (2005, January 1). Review of the port security grant program. (OIG Publication No. 05-10).

U.S. Department of Homeland Security, Office of the Press Secretary. (2003, June 12). Protecting America's ports [Press release]. Retrieved from http://ntl.bts.gov/lib/23000/23300/23328/Port_Security_Press_Kit_DHS.pdf.

U.S. Department of Homeland Security, Office of the Press Secretary. (2003). Protecting America's ports: maritime transportation security act of 2002 [Press release].

U.S. Department of Homeland Security, Transportation Security Administration & U.S. Coast Guard. (2006, June 1). Transportation Worker Identification Credential (TWIC), Consolidation of Merchant Mariner Qualification Credentials (MMC), Joint TSA/USCG NPRM Public Meeting Presentation [PowerPoint slides]. Retrieved from https://epic.org/privacy/surveillance/spotlight/0706/pp0506.pdf.

U.S. Department of Homeland Security, Transportation Security Administration. (2011, July 6). Transportation Worker Identification Credential (TWIC) Program, 2011 Chemical Sector Security Summit [PowerPoint slides]. Retrieved from https://www.dhs.gov/xlibrary/assets/coast-guard-regs-plostock-m.pdf.

U.S. Department of Homeland Security, Transportation Security Administration. (n.d.). TWIC®. Retrieved on February 2016 from https://www.tsa.gov/for-industry/twic.

U.S. Department of Homeland Security, Transportation Security Administration. (2004, November 17). TSA launches prototype phase of new biometric ID card for transportation workers [Local press release]. Retrieved from https://www.tsa.gov/news/releases/2004/11/17/tsa-launches-prototype-phase-new-biometric-id-card-transportation-workers.

U.S. Department of Homeland Security, U.S. Coast Guard, Area Maritime Security Committees. (2013, December 20). Challenges, accomplishments, and best practices – annual report. Retrieved from https://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Report%2020DEC13.pdf.

U.S. Department of Homeland Security, U.S. Customs and Border Protection. (n.d.). Cargo Security and Examinations. Retrieved on 2016, June 10 from https://www.cbp.gov/border-security/ports-entry/cargo-security.

U.S. Department of Homeland Security, U.S. Customs and Border Protection. (n.d.). CSI: Container Security Initiative. Retrieved on 2016, June 10 from https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief.

U.S. Department of Homeland Security, U.S. Customs and Border Protection. (n.d.). C-TPAT: Customs Trade Partnership Against Terrorism. Retrieved on 2016, June 10 from https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism.

U.S. Department of Homeland Security, U.S. Customs and Border Protection. (2015). Vision and Strategy 2020. Retrieved from https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf.

U.S. Department of Homeland Security, United States Coast Guard. (n.d.). Missions: maritime security. Retrieved from http://www.uscg.mil/top/missions/MaritimeSecurity.asp.

U.S. Department of Homeland Security, United States Coast Guard. (2011). Safety, security and stewardship [White paper on the U.S. Coast Guard]. Retrieved from https://www.uscg.mil/history/docs/dhs/dhs_cgwp_2011.pdf.

U.S. Department of Homeland Security, United States Coast Guard. (n.d.). Missions: Maritime Security. Retrieved on 2016, June 10 from http://www.uscg.mil/top/missions/MaritimeSecurity.asp.

U.S. Department of Homeland Security. (2003, February). The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (NS-PPCIKA).

U.S. Department of Homeland Security. (2004). National response plan. Retrieved from http://fas.org/irp/agency/dhs/nrp.pdf.

U.S. Department of Homeland Security. (2005, October). National plan to achieve maritime domain awareness for the national strategy for maritime security. Retrieved from https://www.dhs.gov/sites/default/files/publications/HSPD_MCSPlan_0.pdf.

U.S. Department of Homeland Security. (2009). Northern California Area Maritime Security Committee Charter. Retrieved from http://www.sfmx.org/support/amsc/AMSCCharter.pdf.

U.S. Department of Homeland Security. (n.d.). Department Six-Point Agenda. Retrieved on 2015, September 23 from https://www.dhs.gov/department-six-point-agenda.

U.S. Department of Justice, Food and Drug Administration Office of Criminal Investigations. (2012, July 25). $100 million customs fraud uncovered; president of San Diego Customs Brokers Association and ten others charged in scheme [Press release]. Retrieved from http://www.fda.gov/ICECI/CriminalInvestigations/ucm313527.htm.

U.S. Department of the Homeland Security, Transportation Security Administration. (2006, May 10). DHS issues proposed rulemaking for Transportation Worker Identification Credential [Press release]. Retrieved from https://www.tsa.gov/news/releases/2006/05/10/dhs-issues-proposed-rulemaking-transportation-worker-identification.

U.S. Department of the Treasury, Committee on Foreign Investment in the U.S. (2010, December 1). Process Overview. Retrieved from https://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

U.S. Department of the Treasury. (2006). CFIUS and the Protection of the National Security in the Dubai Ports World Bid for Port Operations [Press release]. Retrieved from https://www.treasury.gov/press-center/press-releases/Pages/js4071.aspx.

U.S. Department of Transportation, Bureau of Transportation Statistics. (Chambers, Matthew. (2010, October). Atlantic Coast U.S. Seaports. Retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/bts_fact_sheets/october_2010/html/entire.html.

U.S. Department of Transportation, Maritime Administration. (2008, May). Glossary of shipping terms. Retrieved from http://www.marad.dot.gov/wp-content/uploads/pdf/Glossary_final.pdf.

U.S. Department of Transportation, Maritime Administration. (2008, May). Glossary of Shipping Terms. Retrieved from http://www.marad.dot.gov/wp-content/uploads/pdf/Glossary_final.pdf.

U.S. Department of Transportation, Maritime Administration. (2013). Vessel calls snapshot, 2011.

U.S. Department of Transportation, Maritime Administration. (2013) Vessel Calls Snapshot, 2011. Retrieved from http://www.marad.dot.gov/wp-content/uploads/pdf/Vessel_Calls_at_US_Ports_Snapshot.pdf.

U.S. Department of Transportation, Maritime Administration. (2015). Factsheet: 2013 Vessel Calls in U.S. Ports and Terminals. Retrieved from http://www.marad.dot.gov/wp-content/uploads/pdf/DS_MARAD-2013-Vessel-Calls-Information-Sheet.pdf.

U.S. Department of Transportation, Maritime Administration. (n.d). About us. Retrieved 2015, September 15 from http://www.marad.dot.gov/about-us/.

U.S. Department of Transportation, Maritime Administration. (n.d.). About Us. Retrieved on 2015, September 16 from http://www.marad.dot.gov/about-us/.

U.S. Marine Corps. (n.d.). Blount Island command. Retrieved on 2015, October 3 from http://www.bic.marines.mil/About.aspx.

U.S. Senate Homeland Security Committee. (2006, February 27). Coast Guard Intelligence Coordination Center assessment of the DPW purchase of P&O [Unclassified document].

United States Maritime Alliance, Ltd. (n.d.). USMX: about USMX. Retrieved on 2015, September 15 from http://usmx.com/about.

United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Improvements Act of 2011, S. 1125, 112th Cong. (2011). Retrieved from https://www.govtrack.us/congress/bills/112/s1125.

USCG port plan to balance security, economics. (2003, June 10). *Dow Jones Newswires*. Retrieved from http://www.sfmx.org/support/amsc/archivedocs/AMSC%20Guide%20to%20Industry%20and%20Law%20Enforcement%20stay%20informed%20of%20DHS%202003.pdf.

van Ham, J.C. (1998). Changing public port management in the Hamburg-Le Havre Range. *Maritime Engineering and Ports*, 36, 13-21. Retrieved from http://www.witpress.com/Secure/elibrary/papers/MAR98/MAR98002FU.pdf.

The White House. (2003 February). The National Strategy for Physical Protection of Critical Infrastructures and Key Assets. Retrieved from https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

The White House. (2012, August 14). National Strategy for Maritime Security: National Maritime Domain Awareness Plan. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/national_maritime_domain_awareness_plan.pdf.

The White House, Office of Homeland Security. (2002). National Strategy for Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

The White House, Office of Homeland Security. (2007). National Strategy for Homeland Security. Retrieved from https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

The White House, Office of the Press Secretary. (2006). Fact Sheet: The CFIUS process and the DP World transaction [Press release]. Retrieved from http://2001-2009.state.gov/e/eeb/rls/fs/2006/61915.htm.

The White House. (1998, May). Presidential Decision Directive/NSC-63, critical infrastructure protection. Retrieved from http://fas.org/irp/offdocs/pdd/pdd-63.htm.

The White House. (2002). The national homeland security strategy of the United States of America. Retrieved from http://www.state.gov/documents/organization/63562.pdf.

The White House. (2003, December). Homeland Security Presidential Directive-7 (HSPD-7).

The White House. (2004). National Security Presidential Directive (NSPD) 41 / Homeland Security Presidential Directive (HSPD) 13.

The White House. (2005, September 20). National maritime security strategy. Washington, DC, 2005. Retrieved from https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html.

The White House. (2006, February). The federal response to Hurricane Katrina: lessons learned. Retrieved from http://www.uscg.mil/history/katrina/docs/KatrinaLessonsLearnedWHreport.pdf.

The White House. (2010, May). National Security Strategy. Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

The White House. (2011, May). National Strategy for Counterterrorism. Retrieved from https://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

White, R. (2011, September 9). Port security goes from an afterthought to a priority. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2011/sep/09/business/la-fi-911-ports-20110909.

Willis, L. (2007). Transportation Trades Department, AFL-CIO [Testimony, Subcommittee on Coast Guard and Maritime Transportation, United States House of Representatives].

Wolff, E. & Koenig, G. (2010). The role of the private sector in emergency preparedness, planning, and response. In Abbott, E. & Hetzel, O. (Eds.). *2nd Edition of Homeland Security and Emergency Management: A Legal Guide for State and Local Governments*. Chicago, IL: ABA Publishing.

The World Bank. (2016). Container Port Traffic (TEU: 20 foot equivalent units). Retrieved on 2016, July 12 from http://data.worldbank.org/indicator/IS.SHP.GOOD.TU.

The World Bank, Public-private-partnership in infrastructure resource center. (n.d.). Graphic explaining the contractual relationships in a "landlord" port. Retrieved 2016 July 16 from https://ppp.worldbank.org/public-private-partnership/library/graphic-explaining-contractual-relationships-landlord-port.

World Shipping Council. (2002, December 5). Comments of the World Shipping Council submitted to the U.S. Department of Transportation, Transportation Security Administration, regarding Operation Safe Commerce. Retrieved online http://www.worldshipping.org/pdf/operation_safe_commerce.pdf.

Wrightson, M. (2005, May). Maritime security enhancements made, but implementation and sustainability remain key challenges [Testimony, Committee on Commerce, Science, and Transportation, United States Senate].

Wytkind, E. (2013, June 18). Time to Reconsider Flawed TWIC Program [Press release]. AFL-CIO, Transportation Trades Department.

York, J., Hargrave, J. & Pacheco, D. (2016). Converging winds: logic hybridization in the Colorado wind energy field. *Academy of Management Journal* 59(2), 579-610 DOI: 10.5465/amj.2013.0657.

Zunes, S. (2006, March 15). U.S. Democrats in dry dock over ports. *Asia Times*. Retrieved from http://www.atimes.com/atimes/Middle_East/HC15Ak02.html.

APPENDIX A – THE EVOLUTION OF CRITICAL INFRASTRUCTURE AWARENESS AND PROTECTION

Efforts to coordinate critical infrastructure protection and promote public and private sector dialogue in the field of infrastructure protection began long before 9/11. Recent policies and national strategies promulgated after 9/11 have a non-definitive starting point in the national consciousness beginning in the late 1970s. Some early public sector work was focused on "ensuring the survival of a constitutional form of government and continuity of essential Federal functions; plans dealt primarily with the threat of nuclear attack" (U.S. Department of Homeland Security, Homeland Security Advisory Council, 2006). Other joint public-private initiatives were focused on cybersecurity. In 1977, for example, the National Information Systems Security Conference (NISSC) was created to encourage discussion of burgeoning cyber and information systems security (Tritak, 1999). The Computer Security Act of 1987 tasked the National Bureau of Standards to create computer standards for federal agencies including a comprehensive security program with benefits foreseen for the private sector (Computer, 1988).

In July 1996, Presidential Executive Order EO-13010 Critical Infrastructure Protection was promulgated declaring "certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (Critical Infrastructure Protection, Executive Order, 1996).

This Executive Order listed the following as critical infrastructures: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government (Critical Infrastructure Protection, Executive Order, 1996). In addition, the Executive Order created the President's Commission on Critical Infrastructure Protection (PCCIP) with a primary focus on emerging cybersecurity issues. The PCCIP was tasked with providing recommendations on next steps for ensuring enhanced critical infrastructure protection. In 1997, the PCCIP passed on its recommendations including calling for greater public-private partnership moving forward (Tritak, 1999).

The recommendations from the PCCIP were then assigned to an interagency working group for further consideration. This process culminated in 1998 with the issuance of Presidential Decision Directive/NSC-63 (PDD-63) by then President William Clinton. PDD-63 recognized American reliance on "certain critical infrastructures and upon cyber-based information systems" (The White House, Presidential Decision Directive, 1998). PDD-63 reinforced the concept that public-private partnership was crucial to eliminating potential vulnerabilities and listed lead agencies in the federal bureaucracy to liaise with the private sector. The lead agency/sector liaisons were:

Lead Agency	**Sector Liaison**
Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	• Aviation

	• Highways (including trucking and intelligent transportation systems) • Mass transit • Pipelines • Rail • Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service; Continuity of government services
HHS	Public health services
Energy	• Electric power; • Oil and gas production and storage

And PDD-63 designated lead agencies for special functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense

Source: (Presidential, 1998)

The same memo directed the departments of Commerce and Defense to lend their expertise to owners of critical infrastructure to "develop security-related best practice standards" and encouraged more communication between the public and private sectors (The White House, Presidential Decision Directive, 1998). At the same time increased communication was being promoted between the public and private sectors, more people were also recognizing the importance of increased communication within the interagency process.

Introduced 6 days before 9/11, the proposed Critical Infrastructures Protection Act of 2001 was not passed but rather incorporated into other forthcoming legislation. Importantly, however, it defined critical infrastructure 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 debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Critical Infrastructures Protection Act, 2001).

A few weeks later, the USA PATRIOT Act was passed and in it is a clarification of U.S. policy on critical infrastructure. Without explaining how, the USA PATRIOT Act read, "(1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States; (2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations"(USA PATRIOT Act, 2001).

The first National Homeland Security Strategy was published in 2002 (2002 Strategy), suggesting the private sector conduct risk assessments and invest in systems to protect key assets. According to the 2002 Strategy, the private sector's "internalization of these costs is not only a matter of sound corporate governance and good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees and the Nation" (The White House, 2002). The 2002 Strategy also outlined how the Department of Commerce's Critical Infrastructure Assurance Office and the FBI's National Infrastructure Protection Center would be consolidated under the

Department of Homeland Security. The 2002 Strategy went on to state that the private sector spent approximately $55 billion a year on private security prior to the September 11th attacks and envisioned a 50 to 100% increase as a result of a prolonged fight against terrorism. Shortly thereafter, the 2002 Strategy envisioned the United States working with its trade partners to increase security at U.S. ports (The White House, 2002).

In February 2003, the White House published its National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003 Strategy). The 2003 Strategy called specifically for better access control at transportation facilities, including workforce identification measures (The White House, 2003).

PDD-63 was eventually superseded after 9/11 with the National Strategy to Secure Cyberspace in February 2003 and 10 months later (December 2003) with a second Presidential Decision Directive using the new nomenclature of Homeland Security Presidential Directive 7 (HSPD-7). HSPD-7 formalized the role of the Secretary of Homeland Security as the national coordinator for critical infrastructure identification, prioritization and protection (The White House, HSPD-7, 2003). HSPD-7 modified the original list of critical infrastructures outlined in PDD-63. The revised sector-specific federal agency list thus read:

Designated Sector-Specific Agency	**Critical Sector**
Department of Agriculture	Agriculture; Food (meat, poultry and egg products)
Health and Human Services	Public health; Healthcare; and Food (other than meat, poultry and egg products)

Environmental Protection Agency	Drinking water and water treatment systems
Department of Energy	Energy including the production refining, storage and distribution of oil and gas and electric power except for commercial nuclear power facilities
Department of the Treasury	Banking and finance
Department of the Interior	National monuments and icons
Department of Defense	Defense industrial base

Other specified agencies were given specific functions as well. Here is a partial list of those agencies and their responsibilities:

Department or Agency	**Specified Responsibility**
Department of State	Work with foreign countries and international organizations to strengthen protection of U.S. critical infrastructure
Department of Homeland Security	Information technology; Telecommunications; Chemical; Transportation systems (Including mass transit, aviation, ***maritime***, ground/surface, rail and pipeline systems); Emergency Services; and Postal and Shipping

Department of Justice/FBI	Domestic terror threat reduction
Department of Commerce	Improve technology for cyber systems and promote other critical infrastructure efforts

Source: (The White House, HSPD-7, 2003).

HSPD-7 also created several infrastructure-related task forces, intelligence fusion centers and a host of other groups, committees and agencies designed to coordinate infrastructure protection.

Additional policies and strategies are discussed in this dissertation's case study.

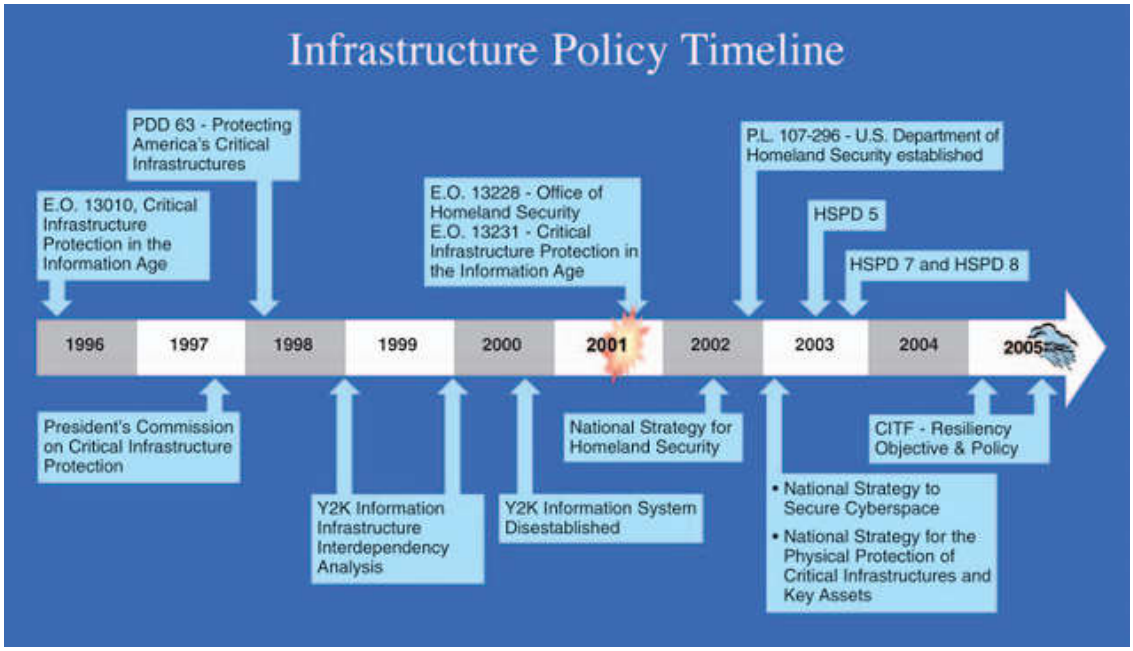


FIGURE A.1. EVOLUTION OF CRITICAL INFRASTRUCTURE POLICY OVER THE LAST DECADE

Source: U.S. Department of Homeland Security, Homeland Security Advisory Council. 2006.

APPENDIX B: SUBJECT MATTER EXPERT INTERVIEWEES

	Profession	*Interview Date*
1	Government security official	12-Feb-16
2	Government security official	12-Feb-16
3	Seaport industry executive	16-Feb-16
4	Trade Association official	16-Feb-16
5	Government security official	19-Feb-16
6	Seaport Terminal Operator	19-Feb-16
7	Government security official	22-Feb-16
8	Trade Association official	22-Feb-16
9	Maritime Security Professional	22-Feb-16
10	Government security official	22-Feb-16
11	Seaport industry executive	22-Feb-16
12	Seaport industry executive	22-Feb-16
13	Government security official	22-Feb-16
14	Government security official	23-Feb-16
15	Security Oriented Attorney	23-Feb-16
16	Seaport Terminal Operator	24-Feb-16
17	Trade Association official	24-Feb-16
18	Trade Association official	24-Feb-16
19	Government security official	25-Feb-16

20	Labor union official	25-Feb16
21	Private Sector Consultant	25-Feb-16
22	Government security official	18-Feb-16
23	Seaport industry executive	29-Feb-16
24	Former government security official	1-Mar-16
25	Seaport industry executive	1-Mar-16
26	Former seaport official	2-Mar-16
27	Trade Association official	3-Mar-16
28	Government security official	3-Mar-16
29	Private Sector Consultant	4-Mar-16
30	Government security official	4-Mar-16
31	Trade Association official	4-Mar-16
32	Seaport industry executive	7-Mar-16
33	Seaport industry executive	7-Mar-16
34	Seaport Terminal Operator	8-Mar-16
35	Seaport industry executive	8-Mar-16
36	Former government security official	9-Mar-16
37	Labor union official	9-Mar-16
38	Former seaport official	10-Mar-16
39	Former seaport official	11-Mar-16
40	Seaport industry executive	11-Mar-16
41	Seaport Terminal Operator	14-Mar-16
42	Trade Association official	14-Mar-16
43	Seaport industry official	14-Mar-16
44	Seaport Terminal Operator	15-Mar-16

45	Private Sector Consultant	16-Mar-16
46	Private Sector Consultant	6-Apr-16

APPENDIX C: PARTIAL LIST OF UNRESOLVED TWIC ISSUES DEVELOPED BY THE NATIONAL MARITIME SECURITY ADVISORY COMMITTEE, JULY 2008

Source: (National Maritime Security Advisory Committee, 2008).

1. **Compliance Dates:** "There is a very strong sense among members of the maritime community that those who spent the time, effort and in some cases a significant amount of trouble, to obtain TWICs early in the process are being financially penalized. Specifically, by the time enforcement begins in April [2009], assuming that deadline is met, some individuals will have had their cards for a year and a half… In short TWIC is a user - funded program; users must not be penalized for working to help TSA meet its goals."
2. **Rail Crews:** "The question about how the TWICs of rail crews are going to be verified still looms large."
3. **Utility Workers:** "A national dialogue is required with regard to TWIC cards for utility workers. The population of these workers is far too great and their need for access too infrequent to require a TWIC, however they often need access for emergency repairs."
4. **External Communications:** "the communications team is not particularly visible. Nationwide, there is a concern about both the trucking and merchant mariner communities and whether they are fully aware of the TWIC requirements, especially owner/operators… NMSAC is also concerned over whether

5. manufacturing facilities are communicating with rail companies regarding whether rail workers who access manufacturing facilities will need TWICs."
6. **Hotlist:** "There is currently no way to validate the "hotlist" against a TWIC card presented for access. Further, there is no software or description of how to "decode" the "hotlist" of TWIC card information. DHS should provide this information. Regulated entities must be provided with an electronic access (direct download, searchable database, or telephonic system) to the national database in order to readily verify the validity of a TWIC that is presented for access. The "hotlist" also needs to indicate whether the TWIC has been denied, revoked, suspended lost or stolen so that the owner/operator can make a decision whether or not to allow a person access. This means that the names and biographical information of anyone who has applied for a TWIC and been denied must be available to all owners/operators on a real time basis so that facilities can choose whether to permit access to these individuals with an escort. When an individual reports a card as being lost or stolen, it should be so noted on the hotlist. … Facilities are still unclear whether unescorted access can be provided to someone who has reported a revoked, suspended, lost or stolen card; this information is necessary for facilities to make risked - based decisions on whether to grant access."
7. **Low Enrollment Numbers:** "Of major concern to all stakeholders are the low enrollment numbers."
8. **TSA / Lockheed Martin Performance:** "TSA is still not delivering cards within the seven to 10 days after enrollment, which was the time frame industry required

and which TSA agreed was a target goal; and the agency is not even reaching the 30 days after enrollment as outlined in the final regulation. Since February of 2007, stakeholders have repeatedly requested information on the performance measures specified in the TSA contract with Lockheed Martin. Most recently, NMSAC made this request at the April 2008 meeting. The Committee also requested a copy of any TSA evaluations of the contractors success/non - success in achieving the stated measures. This has yet to be provided."

9. **TWIC Use at Airports:** "It is difficult to understand why TWIC is not universally accepted as an approved federal identification card at all airports. TSA should correct this immediately. There should be a specific deadline date set (and met) after which all airports will accept TWIC as an acceptable form of ID."
10. **Mariner Use of TWIC**: "TWIC should also be an accepted form of identification for pre - employment or random drug testing at testing centers for mariners."
11. **Who Must Obtain a TWIC:** "While the intent of Congress in enacting the Maritime Transportation Security Act of 2002 (MTSA) was clear in requiring that individuals who work on regulated vessels or in regulated marine facilities obtain TWICs, current regulations suggest but do not enumerate the specific job titles of individuals that are required to obtain TWICs.
12. **Law Enforcement Guidance**: "Specific guidance needs to be provided to state and local law enforcement officials on exactly what actions they can and cannot take when a fraudulent or tampered with TWIC is presented. Is it a crime to present a fraudulent card and should that individual be detained, or should the TWIC simply be confiscated? And by whom?"

13. **TWIC Verification at Non-MTSA Facilities and Vessels:** "Equally unclear is what, if any, action a police officer can take if a fraudulent or revoked TWIC is presented as ID at a non - MTSA regulated facility."
14. **Failure to Capture Biometric:** "The USCG and TSA need to assess what the impact on daily operations will be if biometrics are unreadable due to lower quality fingerprint capture."
15. **Escort Requirements:** "While neither the MTSA, Coast Guard regulations implementing TWIC, nor other general land - based law enumerates any potential liability for a TWIC - holder who acts as an escort for a non - TWIC holder who then engages in a transportation security incident or other prohibited act, there have been indications that such liability is contemplated. It is imperative that this matter be clarified. The answer could impact the willingness of certain individuals to act as an escort."
16. **Card Design**: "The TWIC program missed an opportunity to provide a visual identifier on the TWIC card for essential non - uniformed port personnel that might require access on local roadways and to the port for critical response and recovery operations."
17. **Enrollment Center Locations:** "In far too many port locations, fixed sites are often far removed from the ports they are designed to service, and/or lack sufficient truck access and/or parking. In addition, centers are often difficult to find and signage is generally lacking."
18. **TWIC Holder Information Changes:** "The process for renewing the PIN number is unclear. Some stakeholders have been told that if an individual forgets

his PIN he must get a new TWIC card. We have also been told that in order to get a new TWIC card, you need to know your PIN number."

19. **Other Issues:**

    a. "There are still individuals who applied at the Port of Wilmington Delaware in October of 2007 who have yet to receive their cards [6 months earlier].

    b. It has been discovered that the encryption of the fingerprints on certain cards was not performed properly which causes the decryption to fail. No one will know the extent of the problem until those cards that have been issued are tested.

    c. It is as yet unclear what impact fingerprinting issues will have on the biometric component of TWIC. It is our understanding that TSA is aware of the fingerprinting issue and plans to deploy more sensitive readers in the hope of reducing the failure rates.

    d. Other technical problems affecting program rollout include:

        i. Enrollment system failure

        ii. Incorrect name or other information on card

        iii. Photos being processed with darkened photos

        iv. Expiration date errors

        v. Security features not printing properly

        vi. Many applicants have reported enrollment processing of several hours or more at enrollment centers. There is little confidence in the validity of Lockheed Martin's stated average wait time

numbers (e.g., 8 minutes). This lack of confidence is based on anecdotal information as empirical data has not been made available. Applicants have reported that multiple visits for both enrollment and activation – in some cases as many as six visits – to enrollment centers have been necessary because of various technical or operational difficulties. This is inexcusable. Reasons for multiple visits include: can't find card; computer is down, internet is down, can't access server, can't write data to card and will have to try again some other day, etc. Extended enrollment times have been provided as:

1. internet slow,
2. system is slow (in several instances data transfer at activation has taken as long as 1 - 2 hours),
3. information must be entered into the system at enrollment even though individual had pre - enrolled,
4. camera (fingerprint scanner, workstation, etc) not working properly."

APPENDIX D – ACTUAL COPY OF COAST GUARD ISSUED FACILITY PLAN REVIEW CHECKLIST

Enclosure (3) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 03-03, CH-2

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number:				OPFAC:	
Facility Name:				Facility Type:	
Reviewer:		QA Reviewer:		MISLE Activity #:	

§105.405 *Format & Content of the Facility Security Plan (FSP)*	*Yes*	*No*
(a) Does the plan follow the order as it appears below?	☐	☐
- If no, does the plan contain an index identifying the required elements and their location?	☐	☐
(1) Security administration and organization of the facility *Does the plan contain a security organization?*	☐	☐
(2) Personnel training *Does the plan contain personnel training procedures?*	☐	☐
(3) Drills and exercises *Does the plan contain drill and exercise procedures?*	☐	☐
(4) Records and documentation *Does the plan contain facility recordkeeping and documentation procedures?*	☐	☐
(5) Response to change in MARSEC Level *Does the plan contain procedures for responding to MARSEC level changes?*	☐	☐
(6) Procedures for interfacing with vessels *Does the plan contain procedures for interfacing with vessels?*	☐	☐
(7) Declaration of Security (DoS) *Does the plan identify DoS procedures?*	☐	☐
(8) Communications *Does the plan contain communication procedures?*	☐	☐
(9) Security systems and equipment maintenance *Does the plan contain security systems and equipment maintenance procedures?*	☐	☐
(10) Security measures for access control, including designated public access areas *Does the plan contain security measures for access control?*	☐	☐
(11) Security measures for restricted areas *Does the plan contain security measures for restricted areas?*	☐	☐
(12) Security measures for handling cargo *Does the plan identify security measures for handling cargo?*	☐	☐
(13) Security measures for delivery of vessel stores and bunkers *Does the plan address the security procedures for delivery of vessel stores and bunkers?*	☐	☐
(14) Security measures for monitoring *Does the plan identify security measures for monitoring?*	☐	☐
(15) Security incident procedures *Does the plan contain security incident procedures?*	☐	☐
(16) Audits and security plan amendments *Does the plan contain procedures for auditing and updating the plan?*	☐	☐
(17) Facility Security Assessment (FSA) report *Does the plan contain a FSA report?*	☐	☐
(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) *Does the plan contain a completed CG-6025 form?*	☐	☐

Note: If two or more of the above questions are marked "No" then the FSP may be returned to the originator for correction before being reviewed. The plan may not be approved if the FSA report or the CG-6025 form is missing.

Source: This is the actual checklist issued by U.S. Coast Guard District 9 and can be found online at: http://www.uscg.mil/d9/msuChicago/docs/FSP_Review.pdf

APPENDIX E – DEFINITIONS OF VARIOUS ELEMENTS OF SECURITY FOR THE FIRM AND THREAT VECTORS

E.1 SECURITY FOR THE FIRM

Corporate security is not a new phenomenon and is found throughout MNCs in various forms. However, the lack of research associated with corporate security has left a gap in its definition. Thus, for the purposes of this research paper, we define corporate security as a holistic MNC function with 20 specific core elements:

- Personal Security - This element is specifically about the needs of the individual employee. This might include issuance of personal weapons, armored vehicles, escorts, counter-kidnapping training, etc. Likewise, personal protective equipment (PPE), oxygen or radioactive monitors, and a host of other equipment might fall under personal security. A firm maintaining a call list of next-of-kin, providing personal defense training, first aid and CPR training, and a host of other personal related issues might also fall under this element.
- Personnel Security – The intent of a personnel security program is to understand who is working for you and who is gaining access to your corporation. Thus, background checks, reference checks, criminal history and even credit records may all be used to ensure a better vision of who the personnel actually are. Personnel security gives the employer as much information about employees, contractors, and any visitors as is legally attainable in their specific jurisdiction.
- Physical Security – This element has everything to do with the physical infrastructure of the firm's facilities. Fencing, mast head lighting, closed circuit television monitoring, access gates, locked doors, fire alarm and sprinkler systems, and intrusion/movement detectors all fall under this element.

- Information Security – This element specifically addresses that information deemed critical to a company's operations. Thus, intellectual property, patented information, various data on operations, sales, maintenance schedules, and a veritable host of other potential sources all fall under information security. As much of this data is increasingly held on electronic storage devices, information security is separate from cyber security. Information security should focus on safeguarding proprietary information.
- Cyber Security – Purposefully separate from information security is cyber security. This constitutes all the computer, server and telecommunications equipment owned or operated by the firm. This includes authorized access control (uploading, downloading and usage), hard points where systems might be accessed either on-scene or remotely, software protection, fire walls, storage and maintenance of electronic data, etc. Of all these elements of corporate security, cyber security has received the most attention in terms of academic research.
- Corporate Governance – Corporate governance as a system of checks and balances is also part of a comprehensive security program. As a means of checking agency, malfeasance, waste or abuse, corporate governance provides a check on the firm's activities and its officers.
- Compliance and Ethics Programs – Also included in a broad definition are these types of programs that serve to educate and familiarize employees with regulatory and legal restrictions as well as ensuring that the firm complies and adheres to given practices.
- Crime Prevention and Detection – This element focuses on the routine crime prevention found where humans operate in firms. Theft, counter-intelligence, counter-espionage, financial auditing, inventory controls and a host of other issues comprise this element. Uniformed security guards at access points, RFID tags on high value items, and verifying inventory are aspects of this element.
- Fraud Deterrence – This element is both internal to the firm and external when considering various contractors and sub-contractors who provide material,

financial, personnel and legal support to a firm. Active programs to protect against fraud, verification of contractual agreements, efforts to detect fraud if it has happened and to mitigate its effects are all found in this category.

- Investigations – This broadly encompasses the investigatory functions of various stakeholders within the company across a spectrum of possible issues. Thus, inspectors general, internal auditors, and compliance officers are all included in this element. Ideally, these activities have the trust and cooperation to act at least pseudo-independently from the firm to ensure as little friction as possible while they are conducting these activities.

- Risk Management – Traditionally understood to be function of the legal and insurance sides of a firm, these activities must also consider a broad range of corporate and financial risk.

- Business Continuity Planning – Sometimes overlooked, this element is essential to maintaining resiliency in the face of adversity. How the firm is able to respond to emergent crises and either continue operations in a timely fashion are key pieces of this element of corporate security. Essential records, reconstitution of functions, and devolution planning are all part of this element, all of which should focus on ensuring the short and long-term resilience of the firm.

- Crisis Management – This is the functional area with a firm that forms either *ad hoc* or in perpetuity for purposes of managing crises and ensuring the response, mitigation, recovery and planning phases of the emergency management cycle are fulfilled for long-term firm viability.

- Environment, Safety and Health – These are routine functions generally overseen by agencies such as the U.S. Occupational Safety and Health Administration that ensure a degree of employee safety in the workplace.

These various elements of corporate security are not clearly delineated at times. We find spillover between elements and a variety of ways in which firms evaluate, plan, implement and resource these functions. Firms' adherence to any or all of these elements varies greatly by industry, by country and by the personal experiences and skills of

various decision-makers with the firm itself. While an ideal, holistic security program might coordinate and resource all of these activities, there is evidence that firms treat security sometimes as an asset and other times an expense. Justification of resourcing these various elements is sometimes met with glad acceptance and at others with begrudging hostility. How much security is enough is an age old question and not one that we will answer in this research. Rather, we are focused on the amalgamation of the aforementioned programs in its various forms when we discuss security at the seaport/industry level. Further research into these elements would provide fruitful insights for firms and public-private partnerships. Nonetheless, for now, we will move on to defining the threats firms/seaports might face in light of this current research.

E.2 Threats and Threat Vectors

One of the most challenging aspects of corporate security is the infinite number of possible threats facing the firm. After all, the tragic events of 9/11 were perpetrated with inexpensive blades in the hands of a few terrorists. Consequently, while the variations are infinite, there are broad categories into which we can assign a multitude of threats. For definition purposes, the threats are those forces (man-made or natural) that can damage or destroy firm assets including physical, cyber, intellectual, and human resources. Threat vectors are the paths these threats take to affect the firm.

From an organizational perspective, then, the following categories aggregate the most common threats facing firms and seaports specifically man-made threats and natural threats.

E.1.a. Man-Made Threats

- Cyber – Any form of electronic activity designed to gain access, deny access, collect data, install spyware, etc. Also included in this would be the hardware-related incidents enabling the aforementioned electronic activity thus installation or substitution of hardware, tapping of lines or transmissions whether by satellite,

wire or fiber optic transmissions, and so on. Threat vectors include electronic, radio-frequency or computer based attacks.

- Espionage – Corporate espionage is a threat designed to either take information and data of a commercial or national security interest or to destroy data, thus keeping the firm from accessing its own information. Likewise, espionage can also be conducted to learn secrets, operations, strategy, and event intent (*e.g.*, the corporate board has decided to purchase a competitor's firm). This activity can be carried out by employees acting as agents, by both public and private espionage professionals or even by disgruntled individuals interested in either hurting the home firm, making a profit or to help competitors/enemy organizations for some other purportedly altruistic purposes.
- Sabotage – This may be conducted internally or form external sources. Disgruntled employees or visitors who purposefully cause harm either through their actions or omission of actions as well as external sources intent on causing harm to the firm. Again, there are myriad ways that this can happen, such as drone activity, mixing up an order, or attacking peripheral aspects of the extended infrastructure or supply chain for a firm.
- Theft – Again, this threat is both internal and external and may take many forms.
- Unauthorized Access/Use of Intellectual Property – This may take the form of downloading data, breaching a safe, planting snooping devices, sifting through mounds of waste to find internal correspondence, among others.
- Civil Disturbances – This threat may include a range of disturbances including riots, excessive gang activity, and demonstrations.
- Armed Conflict – Is a very real threat both in terms of formal hostilities between warring parties or guerilla activity between non-state actors and others.
- Terrorism – Terrorism are those incidents designed to sow fear and cause damage amongst the public-at-large. Asymmetric and littoral warfare coupled with the rise of non-state actors have seen the private sector increasingly pronounced as legitimate targets by those who would attack both symbolic and real institutions. All of the firms' assets are potential targets with respect to terrorism. People,

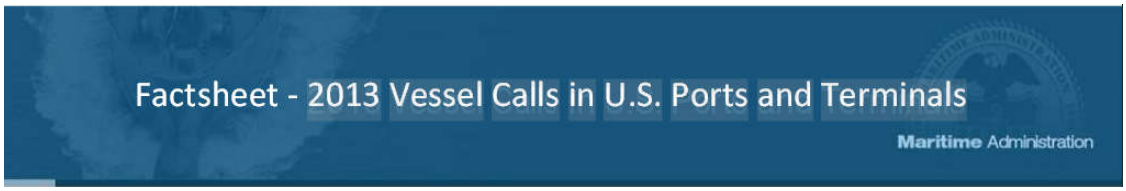
customers, financial stability, physical assets, and even stock prices are targeted by terrorists.

- Other Criminal Acts (including arson) – This category is designed to catch all those other criminal acts that might not be accounted for otherwise.

E.1.b. Natural Threats

- Hurricane/Cyclone – The potentially catastrophic nature of hurricanes coupled with their consequent disruption of normal business activities and critical infrastructure function create formidable threats for firms in regions where these storms occur.
- Dust Storm – Where applicable, these phenomena can cause damage, disruption and loss of income.
- Lightning/Accidental Fire – Whether damaging to electrical or electronic systems, lightning and fire in general have the potential to cause catastrophic damage and severe loss of capability and data.
- Flooding – As we saw in New Orleans following the collapse of the dike in the aftermath of Hurricane Katrina, flooding can cause widespread disruption of activities and critical infrastructure at a time when these are needed most.
- Solar storms – New research in this area coupled with the widespread diffusion of electronic assets create very real threats to some industries and require necessary precautions be taken.
- Tsunami – Similar to other disasters, the force of a tsunami is sufficient to destroy and disrupt. The aftermath may take months or years for a region to recover.
- Earthquake – Similar to tsunamis, the affected area is usually widespread and may take lengthy periods of time to recover.

APPENDIX F – FACTSHEET, 2013 VESSEL CALLS IN U.S. PORTS AND TERMINALS



This Factsheet was produced by the U.S. Maritime Administration (Factsheet, 2015).

Introduction: This is a report containing a calculation of vessel calls for privately owned, oceangoing merchant vessels of all flags of registries over 1,000 gross register tons (GRT) calling at ports and selected ports/terminals within the contiguous United States, Hawaii, Alaska, Guam and Puerto Rico. Though the Maritime Administration strives to provide the most accurate information on vessel activity in the United States, these numbers may vary from statistics collected by port authorities and terminal operators.

What is a privately owned, oceangoing merchant vessel and how is the report derived? We first take a list that contains over 110,000 privately-owned, oceangoing merchant vessels registered with an International Maritime Organization (IMO) number through IHS Maritime and isolate cargo carrying vessels from all other types of vessels utilizing the "Statcode." From this list, we eliminate all passenger and passenger/ro ro cargo ships. We then take this list of vessels and compare it against the Automatic Identification System (AIS) data generated for that vessel.

For more information about Statcode, please visit IHS at this website:
http://www.ihsfairplay.com/about/imo_standards/Setting_Industry_Standards.pdf

For more information about the Automatic Identification system, please visit the United States Coast Guard Navigation Data Center:
http://www.navcen.uscg.gov/?pageName=AISmain

Vessel Types: MARAD uses six vessel categories in this report: (1) Containerships, (2) Tanker, (3) Dry Bulk, (4) General Cargo, (5) Roll On – Roll Off (Ro Ro), and (6) Gas. The following contains the specific vessel types under these six vessel categories:

- Containership – Container Ship and Passenger/Container Ships

- Tankers – CO2, Chemical, Chemical/Oil, Wine, Vegetable Oil, Edible Oil, Beer, Latex, Crude Oil, Oil Products, Bitumen, Coal/Oil, Water, Fruit Juice, Molasses, Glue, Alcohol, and Caprolacatam.
- Dry Bulk – Bulk, Ore, Bulk/Oil, Ore/Oil, Self□Discharging Bulk Carrier, Cement, Wood Chips, Urea, Aggregates, Limestone, Refined Sugar, and Powder.
- General Cargo – Livestock, Refrigerated Cargo, General Cargo, Palletized Cargo, Deck Cargo,
- Passenger/General, Heavy Load, Barge Carriers, Nuclear Fuel, and Pulp Carriers.
- Roll On – Roll Off (Ro□Ro) – Ro□Ro Cargo Ship, Vehicles Carrier (Pure Car□ Truck Carriers),
- Container/Ro□Ro, and Landing Craft.
- Gas – Liquefied Petroleum and Liquefied Natural Gas Carriers

Calls are calculated by how many times a vessel arrived at a port, facility or terminal. This number may include berth shifts, movement to and from an anchorage while awaiting cargo or may include other activities related to vessel, port or terminal operations. Calls do not include vessels arriving at a designated anchorage area.

Capacity is calculated as the sum of vessel calls weighted by vessel deadweight (DWT). DWT is defined as the total weight (metric tons) of cargo, fuel, fresh water, stores and crew which a ship can carry when immersed to its load line. Capacities are also expressed in Twenty Foot Equivalent Units (TEU) for containerships and cubic meters (CM) for gas carriers. An example of overall calls and capacity for a port is provided below:

	# of Calls	DWT	Calls x DWT
Vessel A	10	25,000	250,000
Vessel B	5	20,000	100,000
Vessel C	10	40,000	400,000
TOTAL	25		750,000 DWT

Port Groupings: Certain port and port areas contain multiple docks and terminals or even port areas. They are defined below:

- Columbia River □ Astoria, Kalama, Longview, Portland, Rainier, Vancouver
- Philadelphia/Delaware River □ Burlington, NJ., Camden, NJ., Claymont, Delair, Delaware City,
- Eddystone, Fairless Hills, Gloucester, NJ., Marcus Hook, Milford, DE., Paulsboro, Philadelphia,
- Reedy Point, Salem, NJ., Tullytown, Westville.
- Port of Greater Baton Rouge □ Baton Rouge, Burnside, Darrow, Donaldsonville, Geismar, St.
- Gabriel and Sunshine
- Port of South Louisiana □ Convent, Destrehan, Garyville, Good Hope, Gramercy, La Place, Norco,

- Paulina, Reserve, St. James, St. Rose and Taft
- Sabine□Neches Waterway □ Beaumont, Nederland Terminal, Orange, Port Arthur, Port Neches,
- Sabine LNG Terminal
- San Francisco Bay Area □ Oakland, San Francisco, Martinez, Richmond, Benicia, Stockton,
- Sacramento, Redwood City

Notes for 2013 & Errata

For 2013 – MARAD is utilizing a different data source for this iteration of the vessel calls report. This data source provides us specific event activity which allowed our analysts to isolate every single call a vessel made in a port. Therefore, the information provided is a more realistic snapshot of vessel activity in the United States.

- Additions in 2013 – Apra Harbor, Guam, Bellingham, WA., and Mayaguez, PR.
- Deletions in 2013 – Ferndale, WA., Galveston Lightering Area, Ingleside (included with Corpus Christi), Point Wells, WA, and the South Sabine Point, Southern California and Southwest Pass Lightering Areas.

Data Sources and Acknowledgments:

Primary Data Source: IHS Maritime Vessel Movements and IHS Maritime Lloyds Maritime Database data files.

Acknowledgements: MARAD would like to thank staff at the United States Coast Guard □ Coast Guard Atlantic Area, Operations Analysis Division (LANT□7) for their assistance in helping MARAD generate this data for this report.

Point of Contact

MARAD Office of Policy and Plans

DATA.MARAD@DOT.GOV

APPENDIX G: VESSEL CALLS (Source: Vessel, 2013).

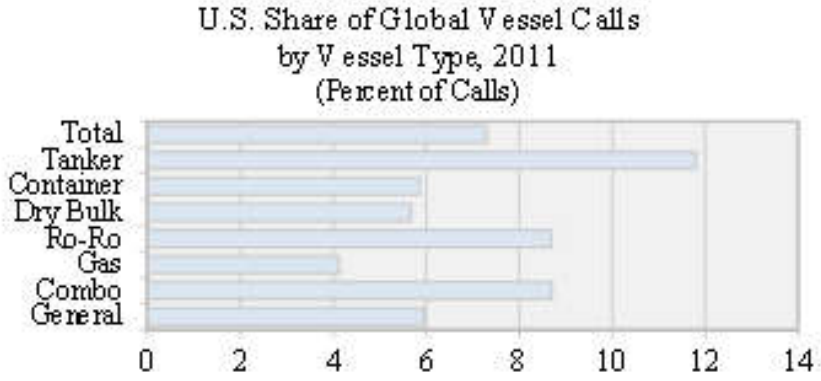
In 2011, the top 10 U.S. ports accounted for 55.5 percent of calls by oceangoing vessels 10,000 DWT or greater (of 132 U.S. ports). Houston was largest for tanker calls; LA/LB was largest for containership calls, and Columbia River Ports were largest for dry bulk calls.

Vessel Calls at U.S. Ports, Top Ten Ports, 2011

Tanker		**Container**		**Dry Bulk**	
Houston	4,652	LA/LB	2,927	Columbia Rvr.	2,193
New York	1,517	New York	2,389	New Orleans	1,195
LA/LB	1,311	San Francisco	2,187	Virginia Ports	1,017
Texas City	1,118	Virginia Ports	2,160	Houston	766
Galv. Light.	969	Savannah	2,015	San Francisco	663
New Orleans	933	Charleston	1,302	Baltimore	610
Galveston	806	Port Ever.	1,075	LA/LB	581
Philadelphia	798	Miami	1,064	Mobile	374
Corpus Christi	747	Houston	827	Tampa	251
San Francisco	681	Seattle	796	Philadelphia	229
Top 10	13,532	Top 10	16,742	Top 10	7,879
All Ports	23,812	All Ports	22,089	All Ports	10,947
Ro-Ro		**Gas**		**General**	
Baltimore	856	Houston	239	Philadelphia	530
Jacksonville	675	Tampa	72	Houston	519
New York	468	Boston	53	New Orleans	248
LA/LB	321	Freeport	50	LA/LB	222
Brunswick	319	Point Comfort	49	Columbia Rvr.	203
Tacoma	315	Philadelphia	48	San Juan, PR	178
Charleston	267	Pascagoula	41	Mobile	167
Philadelphia	243	New Orleans	40	Baltimore	151
Virginia Ports	243	San Francisco	26	Port Ever.	131
Columbia Rvr.	240	Port Arthur	24	Jacksonville	124
Top 10	3,947	Top 10	642	Top 10	2,473
All Ports	6,182	All Ports	857	All Ports	4,029
Combo		**All Types**			
Virginia Ports	34	Houston	7,218		
Houston	27	LA/LB	5,364		
Mobile	17	New York	4,661		
Baltimore	14	San Francisco	3,752		
New Orleans	7	Virginia Ports	3,671		
Corpus Christi	5	New Orleans	2,942		
Philadelphia	3	Columbia R.	2,920		
Lake Charles	2	Savannah	2,731		
Annapolis, MD	1	Philadelphia	2,310		
Freeport	1	Baltimore	2,158		
Top 10	111	Top 10	37,727		
All Ports	120	All Ports	68,036		

Vessel Calls (continued)

In 2011, U.S. ports accounted for nearly 7.3 percent of global vessel calls. The U.S. ranked second in terms of overall calls. Tanker calls at U.S. ports accounted for nearly 12 percent of global tanker calls



Global Vessel Calls by Country, 2011

Country	Tanker	Cont.	Dry Bulk	Ro-Ro	Gas	Combo	Gen.	Total
China	10,698	71,847	31,960	1,943	457	196	6,409	123,510
U.S.	23,812	22,089	10,947	6,182	857	120	4,029	68,036
Japan	4,933	25,227	14,584	6,822	2,084	38	6,784	60,472
Singapore	11,657	16,561	12,520	1,963	967	123	2,391	46,182
S. Korea	6,340	16,224	8,083	3,440	1009	64	2,918	38,078
Brazil	6,169	9,819	8,881	1,260	197	70	2,102	28,498
Italy	7,212	8,888	2,230	5332	373	22	1,622	25,679
Malaysia	5,556	15,995	1,732	268	586	89	1,177	25,403
Taiwan	3,241	14,577	5,597	246	408	13	1,163	25,245
Australia	3,238	4,425	12,830	1,715	460	42	1,564	24,274
Top 10	82,856	205,652	109,364	29,171	7,398	777	30,159	465,377
All Other	118,785	170,737	83,428	41,926	13,370	601	37,571	466,418
Total	201,641	376,389	192,792	71,097	20,768	1,378	67,730	931,795