Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Edmund Levy

has been found to be complete and satisfactory in all respects,

and that any and all revisions required by

the review committee have been made.

Review Committee

Dr. David Gould, Committee Chairperson, Management Faculty

Dr. Lilburn Hoehn, Committee Member, Management Faculty

Dr. James Bowman, University Reviewer, Management Faculty

Chief Academic Officer

Eric Riedel, Ph.D.

Walden University

2015

Abstract

Interagency Coordination of Security Operations in a Large U.S. Seaport

by

Edmund B. Levy

MBA, Pepperdine University, 1977

BBA, University of Texas (Austin), 1970

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Science

Walden University

May 2015

Abstract

Protecting U.S. transportation hubs against a wide variety of security threats, while avoiding undue interference with the normal operations of the hubs, is one of the greatest challenges facing security agencies. The problem addressed in this study was the limited information on the contributing factors to seaport security. The purpose of this case study was to explore issues that can inhibit efficiency of security agency operation and collaboration and to identify actions that have enhanced collaboration. Based on theories of organizational development, leadership, and security tradecraft, this study examined the activities related to maintenance of security at a large California seaport. Research questions focused on the types of relationships that exist among supervisors and employees, how these relationships were formed, types of conflicts among organizations, and methods of task allocation among agencies. Individuals who worked for security agencies were randomly selected for participation ($n = 20$). Data gathering was primarily through face-to-face interviews in an open-ended format and augmented by observations of people working within the research environment. An inductive approach to data collection, with open and axial coding, was used to identify themes and patterns. Key findings included themes of trust among seaport security personnel and threats such as smuggling, sabotage, and terrorism. Conclusions and recommendations may help security officials improve the efficiency and effectiveness of security resources. Positive social change may result from enhanced measures that increase security while avoiding threats to commercial activity and individual civil liberties.

.

Interagency Coordination of Security Operations at a Large U.S. Seaport

by

Edmund B. Levy

MBA, 1977 Pepperdine University

BBA, University of Texas, Austin 1970

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Science

Walden University

May 2015

Dedication

This work is dedicated to the men and women whose diligence and professional dedication continue to provide the rest of our society with the safe and secure environment that is indispensable to our way of life.

Acknowledgments

To the members of the various security organizations who provided me with the information and insights that enabled me to complete this study, I offer my sincere gratitude. In addition, I thank the Walden faculty members and staff who have guided and assisted me throughout my time in the Walden PhD program. My special thanks go to my faculty mentor and committee chair, Dr. David Gould, and to my methodology professor and committee member, Dr. Lilburn Hoehn, as well as Dr. James Bowman, for his assistance through the university research review process.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Threats to the safety of port facilities in the United States have grown to alarming proportions and are increasing. Malevolent parties are growing in violence and ingenuity, with the result that decreased economic activity and the deaths of innocents are substantial possibilities. Port security has, of course, always been a major requirement in any seaport, and various means for providing that security have existed for generations. Since the attacks on U.S. soil of September 11, 2001, the nature of the threat and the complexity of the security task have become both greater and more urgent. U.S. seacoast facilities are subject to jurisdictions of more than one official agency, and each agency has its own capabilities and priorities. This situation, while necessary, complicates the tasks of providing seamless security. To overcome the complications, close coordination among agencies across jurisdictional boundaries is required. The degree to which this coordination has been successfully implemented and maintained offers an interesting and useful topic of investigation.

This chapter includes a general background of the issues of interest as well as of the problems that have been addressed. This is followed by descriptions of the general purpose, nature, and procedures employed in this research study. The scope, assumptions, and limitations are also described. Finally, the significance and potential further use of the study are delineated.

Background of the Study

Existing research and theory literature have provided substantial material related to various issues in the study. Even so, there is a lack of key information about the specific action of theoretical models in the field of interagency collaboration among organizations charged with security at large transportation hubs. Some studies, such as Lisle (2013), indicated that there were problems with conflicting interests and priorities in these kinds of facilities, but the dynamics of the conflicts were not well understood, and the means of resolving them had not been adequately explored. Chalk and Rosenau (2004) noted that U.S. security environments were especially complicated because of the multiple agencies, overlapping jurisdictions, and differing policies, procedures, and ethical rules. In general, Eriksson and Rhinard (2009) observed many of the kinds of issues that are of interest in this work and concluded that much more research will be needed to fully identify, comprehend, and mitigate the issues.

My preliminary approach of some personnel working in the selected research environment revealed that participants would be both available and willing to take part in such a study. In addition to the availability of participants, there also proved to be a plentiful supply of documentary data to inform and guide the design and conduct of the study. The data included books written by experts in various aspects of the study and articles describing research that was useful in defining the need for the current study, for constructing the study, and for evaluating its findings. Despite the availability of supporting theory and research data, current practitioners in the research environment, as

well as researchers who have conducted related studies, have acknowledged that greater understanding of the dynamics of security activity is needed. In addition to the access that has been provided in support of the study, this research has been shown to be both necessary and practicable. For example, Dulles (2006) explained that there are certain things that need to be known in any threat situation before appropriate courses of action can be determined. Most of these pieces of information can only be discovered through field research in the environments where they are relevant. Aydinli (2010) found that the sociology of terrorism and of counterterrorism, as new fields of study, were in need of substantial further examination and research. It thus followed there existed both opportunity and need for such studies.

Variety of Threats

The variety of threat sources as well as threat types greatly complicates the difficulty of preparing to detect and neutralize the threats (Eski, 2011). In addition to many types of terrorist threats, there are also other criminal activities, ranging from simple tariff-avoidance smuggling to transportation of illegal immigrants, importation of proscribed materials, and theft of cargoes. These and other potential crimes add to the complexity of the security task and require the participation of numerous intelligence and enforcement agencies.

According to the content of the Infrastructure Liaison Officer (ILO) training program, operated by the Department of Homeland Security (DHS), there were more than 12 different types of security threats, with more than 60 different origins of the threats

facing U.S. infrastructure facilities. Feldt et al. (2013) listed these threat types along with descriptions of some origins and motivations of those who pose these threats. Most of these threats focus specifically on transportation hubs such as seaports. Sandoz (2012) described the international nature of the threats and the complexities involved in assessing them. Caldwell (2012) related the threats to the kinds of responses that DHS should be structured to make in the face of this wide variety of threats. At the same time, the task of addressing these threats must be done within the context of continuing, efficient operation of the protected facilities. Alitok (2011) offered a description of this dichotomous condition: "Maintaining efficient port operations sometimes conflicts with port security measures addressing worldwide concerns about terrorism, drug smuggling, and crime" (p. 1).

Belzer and Swan (2012) provided one example of the complexity of the task of assessing the threat. This analysis examined the potential effects of low-wage transport workers' vulnerability to economic temptation combined with the increasing possibility (and increasing incidences) of smugglers or terrorists gaining access to shipping containers after they have been loaded and before they reach their destinations. Security personnel must be aware of these kinds of possibilities, devise means of combating the various techniques that can be used to access containers in transit, and do so in a manner that does not unduly hamper the process of transporting the suspect container (and all the others on the same ship). This can be a daunting task, but much depends on its successful completion.

Moreover, the task must be completed, day in and day out, while the normal course of commerce continues. Additionally, this is only one aspect of the security task that the responsible agencies must carry out on an ongoing basis. This example, along with many other types and sources of threats, constitute the collective job of all participating agencies.

Mix of Agencies

To help rationalize the disparate agencies that must be involved, the US Deartment of Homeland Security has implemented a new collection of management processes, known by the general term of collaborative public management (CPM), and has shown some limited promise in helping to reconcile differences in political, institutional, and professional objectives and approaches for achieving security in and around transportation hubs (Garrett, 2010). According to Garrett's study, there were benefits to be gained through implementation of interagency networks, but there were also problems associated with them. Such implementations were seen to offer opportunities for collaboration, but also opened issues associated with organizational rivalries, interference with existing cooperative protocols, resistance to changes in policies and procedures, and assignment of people to tasks for which they may not have had sufficient training or experience. The indications were that the benefits of interagency networks must be gained in order to successfully deal with growing security threats, but that further study of the dynamics of implementation were needed before such large-scale integrative actions could fully yield their intended benefits.

Disparate Ethical Standards

Another critical issue concerned differences in ethical standards and rules among organizations. Even when general ethical principles are held in common, specific rules for upholding these principles may differ from one organization to another, with the potential for real or perceived violations of ethical standards. Such violations can undermine internal morale and cooperative spirit, diminishing public confidence in the agencies involved. Adams and Balfour (2010) studied one such type of clash of ethical rules involving differences between ethical expectations of security personnel who were direct employees of government agencies and employees who were members of organizations that provided contract services to the government. Although Adams and Balfour focused on contract services, their findings revealed potential problems that can occur between government and nongovernment entities as well as within interagency networks of government organizations. A key finding was that it was possible for security organizations to comply strictly with the letter of the law while operating in ways that were counter to some goals of the greater, combined organizations. This fact emphasized the difficulty of establishing governing rules for disparate organizations when those who make the rules may lack detailed understanding of the functional nature of the governed organizations while members of the governed organizations do not possess full understanding of the intent of the new rules to which they are subject.

The issue of ethical rules that may not be held in common among participating organizations may be an additional confounding factor in efforts to establish closely

coordinated action to provide security in transportation hubs. Compliance with general ethical standards and specific rules for gathering and disseminating security data may also conflict with other kinds of ethical standards, as well as conflicting with operational imperatives involving public safety. Such conflicts were identified and explained by Olson (2006) and proved to be significant factors for consideration in the current research project. In addition to honoring internal and interagency protocols, security practitioners were shown to face frequent conflicts between operational, public safety, and societal needs and norms.

The line between legitimate, effective counterintelligence activity and the protection of civil liberties is often obscure (Olson, 2006). Although there are myriad laws and regulations in place to help manage this inherent conflict, dynamic security situations have often challenged even the most conscientious security practitioner. Even so, given the indispensable nature of public cooperation with and faith in the security agencies and activities, maintaining ethical standards and public perception of those standards is imperative for all security practitioners. When conflicts—even innocent conflicts—among agencies come into public view, public confidence can be undermined. Thus, both the fact and appearance of strict ethical practices have continued to be vital to effective execution of security operations.

Roles and Responsibilities

In addition to potential ethical misunderstandings, the mere task of developing detailed descriptions of roles and responsibilities for the various agencies involved in

local area security can be far more difficult than originally envisioned. According to Oliver (2009), establishment of umbrella organizational structures may be reasonably achievable if sufficient funding is provided and if all participating agencies concur that there is benefit to be gained. Even so, Oliver found that general agreement on the basic structure and hierarchy of such organizations did not result in effective and unequivocal division of tasks, or full and detailed understanding of roles, responsibilities, and authorizations to act. Oliver described the goal of defining such roles as both elusive and contradictory.

The elusive nature of such definitions resulted from a variety of factors, including differences in legal definitions of terms, differences among laws and policies across jurisdictional lines, interorganizational rivalries, and failures of communication in the process of constructing the larger organization. Although official efforts to clarify and remove conflict from roles and jurisdictional boundaries have continued, conflicts have continued to arise, and such conflicts unavoidably cause disruption, confusion, and diminution of trust. Any actions that have helped to reduce incidences of these kinds of conflicts should be identified and described to help those responsible for managing jurisdictional boundaries to also maintain cooperative spirit in the process.

Existing Relationships

Finally, establishment of newly chartered organizations can be impeded by existing relationships. In the absence of formal, interagency relationships, it is not unusual for individuals and small groups from different agencies to develop their own

cooperative protocols. Such working protocols may complicate the task of formalizing distribution of roles and responsibilities, especially when high-level officials who may not be aware of the working-level arrangements that already exist negotiate the structure of the formal organization. Division of task through negotiation is generally as much political as practical, influenced by competition for resources, jurisdictional ambiguities, and other factors that may not be visible to personnel who are accustomed to focusing on immediate, working-level tasks.

According to Chenoweth and Clarke (2010), such factors can prove to be confounding if not identified and dealt with in a manner that fosters substantial communication, both vertical and horizontal, throughout the affected organizations. The higher the level of ultimate authority, the more difficult it can be to achieve efficient and effective cooperation among lower-level agencies. Fostering of cooperative relationships "among multiple jurisdictions and actors to overcome this collective action problem is proving more difficult than anticipated by national policy makers" (Chenoweth & Clarke, 2010, p. 495).

This same study also revealed that sensitivity to capabilities, preferences, and habits within lower level agencies is indispensable to successful integration of individual organizations into an effectively functioning whole. Failure of authority figures to recognize existing power structures and roles is a recurring source of difficulty. Successful integration, then, would seem to depend upon recognition and accommodation of existing relationships, even while satisfying political and administrative imperatives

that are associated with higher-level policy, externally imposed demands, and negotiated allocation of funding.

Mix of Issues

Thus, establishment of new interagency organizations for combining security resources places substantial requirements on political and administrative leadership. Understanding of all potential threats is, of course, essential, but this is only one facet of a complex set of issues. It is also necessary to understand the capabilities and limitations of all of the agencies that may be called upon to contribute to the common security program. Sensitivity to the many local pressures and expectations of participating agencies and the specific communities they serve is also indispensable to effectively organizing the network of organizations. Effective negotiation is vital but must be conducted within a context of existing relationships and working protocols.

All of these issues must be identified and comprehended in order to build the kinds of organizational relationships that will optimally employ the many, varied resources that will be needed to face and defeat the growing variety and sophistication of security threats that confront the U.S. transportation infrastructure. It is vital for all concerned to remain cognizant of the fact that security agencies are made up of people in the same way as any other type of organization. Snyder (1993) explained that existence of official direction and policy did not substitute for onsite management and motivation of individuals in the organization. Chalk and Rosenau (2004) elaborated on some of the types of real-time issues and organization-specific processes that tend to spread the need

for active management and control throughout all levels of security organizations. The issues and challenges associated with building and motivating these groups of individuals remain the same ones that managers of other organizations face, with the added dynamic of responsibility for the safety and security of everyone in their operating environment.

Problem Statement

The problem was that there is limited information regarding the contributing factors to seaport security. Port security operations, while vital to the continued, safe operation of port facilities, also entail activities and restrictions that have the potential of interfering with the very functions at the port that the security organizations exist to protect. Maintenance of physical security in the study site seaport is a task that exemplifies the larger issue of security in the entire United States (Sandoz, 2012). The imperative of protecting lives and property from a wide range of potential threats while avoiding undue interference in the ongoing functioning of the affected facilities is a complex, expensive, and unpredictable requirement. These imperatives have motivated an increasingly centralized, hierarchical management structure under the primary direction of the U.S. Department of Homeland Security (DHS).

Under this organization, state and local security organizations have been partially funded and their functions incorporated into a large, collaborative group, with each making its own contribution while remaining answerable to its own individual command and political structures. Absence of any major breaches of security would seem to indicate that the new arrangement is working successfully, but the question remains

whether the new processes are superior to the informal relationships that previously existed (and that may still exist) among some members, given that security breaches did not occur while they were in place (Kempfer, 2011). Thus, identification of some of the organizational dynamics that have resulted in the successful melding of existing relationships in the research environment could help to enhance and further develop the collaborative operation. In addition, detection and description of any remaining difficulties and potential remedies may help build upon this effort.

Purpose of the Study

The purpose of this qualitative case study was to explore issues that can hamper efficiency of security agency operation and collaboration and to identify actions that have enhanced collaboration. To do this, I have explored the activities of security agency personnel and such others as were considered appropriate to discover factors that are associated with collaboration within the study environment. The objective of these observations and enquiries was to explore the perceptions of participants regarding the implementation of interagency collaboration protocols. Corollary explorations included observations of collaborative activities involving members of diverse agencies with similar or compatible security goals, in order to identify modes of behavior that indicated the kinds of relationships that existed among participants.

The central issue pursued was the nature of the collaboration and the manner in which participants were observed to interact. Using interviews, augmented by observations of ongoing operations and examination of official documentary guidance,

the study objective was to identify the kinds of interactions intended by the participants, the interactions I observed, and the official doctrine that was intended to govern the interactions.

The objective was to assess the kinds of collaborative activities that occur and to identify factors that tend to enhance or hinder collaboration. Finally, I interviewed facility users, such as commercial operators, regarding perceptions of the people whose safety is the purpose of the security operations. The study included evaluative conclusions about the manner in which interagency collaboration was taking place, factors that seemed to facilitate the collaboration, factors that hinder collaboration, and potential remedies for problem areas that have been identified.

Research Questions

There were three principal questions addressed in this study. They concerned the nature of professional relationships that were intended to be established, the hierarchical arrangement of decision authority, the nature and extent of existing working relationships in the operating environment, and the manner in which security relationships were to be maintained in a way that avoids disruption to the purposes for which the port exists.

RQ1: What security-related working relationships exist among all observable entities within the research environment?

RQ2: How have informal working relationships formed and what factors have kept them functioning?

RQ3: What kinds of security threats were recognized within the research environment and how were they identified and assigned for action?

Conceptual Framework

The conceptual framework was informed by the work of Schein (2010), who described factors affecting development of organizational cultures and the role of leadership in forming them. Schein discovered that as organizations coalesce, they develop cultures that are unique to them and that these cultures affect the manner in which the purposes of the organizations are pursued, the manner in which members interact within the organizations, and the effectiveness of the organizations. Schein further asserted that a major influence on the development of organizations was the action of individual leaders who guide, inform, and motivate members to behave and interact in particular manners.

In the context of this study, Schein (2010) provided concepts that were reflected in studies of specific phenomena related to the study environment and the unique organizational issues inherent in it. For example, Chalk and Rosenau (2004) described in detail the complexities inherent in the tasks of mitigating security threats within the United States as compared to similar situations in other democratic countries. The principal issue affecting the U.S. security environment much more than that of the other countries was the existence of multiple, independent levels of governmental agencies with varying security-related tasks. These various agencies have differing jurisdictions, many of which overlap: varied priorities, multiple policies and procedures, and disparate,

often conflicting political motivations. The general organizational and leadership dynamics described by Schein (2010) provided a sound basis upon which interactions in the research environment have been observed and interpreted. Additionally, there are multiple skills and capabilities required for maintaining security in dynamic environments, especially those involved in international commerce and transportation. Johnson (2009) and Dulles (2006) described many of these in detail, and no single individual can possess all of them.

This range of required individual capabilities, combined with the multiple agencies in which they exist, makes the task of maintaining security in a large transportation hub especially complex. Even so, the fact that the organizations involved in security operations at the subject seaport have found ways to cooperate on activities that require mutual participation, clarify jurisdictions, and optimize use of resources indicated that some sharing of task and talent was likely to be taking place.

Lisle (2013) presented an argument that the complex interrelationships required for effectively combating terrorism necessarily encompassed all stakeholders. This meant that everyone from street-level enforcement operatives to tourists on holiday needed to be included in the preparations, precautions, and cooperation required to enhance their mutual security. Some of these activities were obvious and visible, such as the extraordinary measures exercised at embarkation points for screening passengers, cargoes, and staff. Others were subtler, but all required some level of participation or at least tacit cooperation from many individuals and groups.

As such, observation and evaluation of factors affecting coalescence of multiple organizations with a common purpose requires recognition of the influence of leaders in the presence of events and individual responses to them. It is this combination of factors, acting within and among the larger interorganizational issues described above, that informed the conceptual framework of this study.

Nature of the Study

This was a case study based primarily on interviews with key individuals from the various agencies having some responsibility for security of the port. Additionally, information was gathered from other individuals who work in commercial or other nongovernmental activities. Early interviews helped identify additional candidate participants. Selection of participants as well as types of questions asked were informed by official documents that influenced or directed interagency operations.

Other data, such as meeting minutes of interagency committees, newsletter articles regarding security operations, or incidents also augmented the interview data and such content from security training programs as was available. Concurrently, the study design included observations of ongoing security activities to establish norms of interaction among individuals and small groups of operatives from the various agencies that functioned in the research environment. From this information, a description of the kinds of interpersonal dynamics among security personnel was formed. This description included interpretations of data that indicated the degree to which personal rather than official cooperative protocols operated within the port environment. Secondarily, the data

served to help reconstruct the manner in which the cooperative relationships were formed.

Definitions

Several terms have specific definitions in the context of this study.

Collaborative public management: A generic term referring to efforts to coalesce the resources and capabilities of multiple agencies to collectively pursue common purposes. In the context of the present study, it refers to coordination of federal, state, and local security agencies. According to Garrett (2010), the expression refers generically to any effort to gain synergistic value among multiple agencies and does not follow from any single policy.

Department of Homeland Security (DHS): A cabinet-level, federal organization with overall responsibility for all aspects of protecting American people and property from a wide variety of threats. Several other agencies, such as the U.S. Coast Guard, operate under direction of DHS.(presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Infrastructure liaison officer (ILO): A person with responsibility for some aspect of facility or personnel security, who is not a member of an official enforcement agency, but who has had specific (DHS provided), training for recognizing potential threats, and reporting them to appropriate authority. (presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Intelligence: Information related to the task of maintaining security. It may concern potential or actual threats, or may be general data that are of use in the security processes. (presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Panga: A type of commercial boat often used by smugglers. Although the name refers specifically to a particular manufacturer's product, Panga has become a generic term for any small vessel used for coastal smuggling or other illicit activities. (presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Tradecraft: A collective term referring to the skills and techniques employed by intelligence operatives in the conduct of their work. It generally focuses on acquisition of intelligence, but may also include the practice of recruiting other operatives, analyzing intelligence, or protecting data or the sources from which it is drawn. (presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Twenty foot equivalent unit (TEU): A measure of ship cargo, usually associated with container ship loads. It refers to an amount of cargo that would fill a standard, twenty-foot long cargo container, and is used as a measure of carrying capacity for ships, as well as a measure of cargo movement through a seaport. (presenter, Infrastructure Liaison Officer lecture, personal communication, October 10, 2011)

Assumptions

A key assumption guiding this study was that participants would not feel any necessity to provide false or misleading answers to questions because they were assured

of confidentiality. The questions were structured to reinforce this expectation, and the participant briefing was designed specifically to assure all participants that their anonymity will be carefully protected. Another assumption was that relationships between individual actions and governing official policy could be observed during the course of their normal working operations, whether these actions were compliant or not.

Scope and Delimitations

Although some relevant activities and events occur outside the area of the subject port facility, most have been excluded from this study. This decision limited the study to the geographical limits of the port and its immediate surroundings. A small number of exceptions were made, such as observations and interviews to be conducted in the adjacent port because the activities and their effects cannot be practically separated from those in the primary area of interest. This exception was applied only to governmental organizations.

Only those civilian organizations and individuals operating within the primary boundaries were included in the research plan. Another delimitation was related to the time limit for the research. Because of the limited span time, some relevant activities did not occur during the conduct of the study. For example, interorganizational diving operations are episodic, occurring only when a mishap or risk occurs. No such events occurred during the time of the study, which meant that cooperation among various dive teams was not available for observation. Seventeen interviews, lasting 1 to 2 hours each,

with observations occurring over approximately 2 months, incidentally excluded opportunities for observing some activities that would otherwise have been of interest.

Limitations

The study was necessarily limited by the degree to which information could properly be provided by the study participants. Even though some extraordinary access was promised, there remained some types of data that had to be excluded, either because of security classification of the data or because of privacy issues. Allowance for these limitations was made in planning the study, and sufficient useful information was still available, facilitating assessment and conclusions.

A further limitation concerned the number and types of organizations that may influence the activities under study. Some governmental issues were not accessible for the research, including legislative and judicial decisions and rulings that remained beyond the control of the participating organizations. The same limitation applied to civilian organizations, such as shipping companies or other users of port facilities, that have their own policies for maintaining security, some of which were not observable during the course of the study. Another limitation is that some of the results may not be generalizable to other similar facilities because of conditions that were unique to the research environment. It is also true that, as the researcher, I already had some familiarity with the environment and with some of the organizations studied, which could be a source of bias. To help avoid this, participants were sourced to avoid including any who

were already familiar, and I did not have any direct involvement with any of the organizations studied (except as they relate to the study itself).

Significance of the Study

With threats to U.S. transportation hubs growing in complexity, variety, and sophistication, there is a corresponding need for increasingly robust measures to counter these threats. These measures must include all relevant domains, ranging from international diplomatic focus on threat detection and prevention, to threat intelligence gathering and dissemination, to mitigation of vulnerability at the sites where security issues may take effect. To fulfill these needs, many kinds of actions and resources will have to be applied.

The focus of this project was on the application of resources at the points where security problems may occur (i.e., the subject port and its immediate environs). Within that particular domain, the specific interest of the study was narrowed to the manner in which existing security resources have been mobilized, coordinated, and directed, as well as the ongoing and future efforts of official government agencies to further enhance the capabilities and effectiveness of existing and recently added security resources. Execution of the research plan revealed some of the recently implemented actions that are proving to add value while avoiding disruption or negation of existing security agency interactions.

I have also discovered that some actions have been counterproductive. These revelations have provided information that should be useful in guiding future actions

associated with increasing the efficiency and effectiveness of security resources at the port. Much of this information should prove to be applicable elsewhere, in which case the conclusions should prove useful to decision makers at other transportation hubs as a source of lessons learned, which could help multiple sites improve the effectiveness of applied resources while avoiding pitfalls inherent in making changes to ongoing operations.

The results were made available to managers of the various organizations involved in the study for their use in making decisions concerning coordination among their own organizations in order to increase efficiency and effectiveness. Because some of the organizations involved work with multiple transportation hubs beyond the research environment of this study, there should also be benefit to organizations at other sites. Finally, the results of this work should contribute to positive social change by helping security personnel recognize the kinds of actions that enhance security while continuing to respect the rights of citizens by avoiding disruption to their legitimate activities. Should any of the lessons learned in this research project be applied as expected at other transportation hubs, this social change benefit will accrue beyond the research environment.

Summary

The study has been conceived and structured to examine the nature of interagency cooperation to maintain security within the research environment. Some longstanding relationships are expected to be altered, superseded, or otherwise affected by emerging

official policy that are intended to codify and clarify these relationships. The study has identified some of the existing relationships, both official and informal, and analyzed the transitions into modified and formalized policies and procedures.

The study has also described the relationships in the context of ongoing commercial and recreational activities. Difficulties and conflicts confronting the various security personnel were a major focus. As a corollary issue, observations of methods employed to mitigate these difficulties and conflicts were also conducted.

A principal outcome of the study has been a set of observations and analyses of practices and techniques that have worked or are reasonably expected to work in helping security personnel efficiently and effectively maintain security in the dynamic environment of this busy, commercial port. The resultant analyses should prove useful to security practitioners within the port environment and may be helpful to practitioners in other transportation hubs that face similar demands and challenges. Chapter 2 includes the review of the literature, and Chapter 3 includes the research methodology.

Chapter 2: Literature Review

Maintenance of physical security in the study seaport is a task that exemplifies the larger issue of security in the entire United States. The imperative of protecting lives and property from a variety of potential threats while minimizing interference in the ongoing functioning of the facilities is a complex, expensive, and unpredictable requirement. The purpose of this qualitative case study was to explore issues that can inhibit efficiency of security agency operation and collaboration and to identify actions that have enhanced collaboration. The objective of these observations and enquiries was to explore the perceptions of participants regarding the implementation of interagency collaboration protocols.

This chapter covers the strategy employed to discover the body of literature related to the study subject. This included literature related to the types of security issues that seaports and other transportation hubs face, theoretical background material related to organizational dynamics and factors of leadership, and procedural guidance for designing and conducting the study. This has been followed by a discussion of literature that informed the conceptual framework.

As the nature of the problem and the purpose of the study are inseparable from the organizational dynamics, selection of the literature for the areas of interest involved interrelated material. This interrelationship, in turn, combined with the nature of the research environment, has provided an unequivocal basis for selection of the research design.

Three types of literature sources have informed the development of the research project: sources related to the security threats affecting the port and the means of combating those threats, sources related to the organizational dynamics that operate in the research environment, and sources that have guided the selection of the research approach and methodology. For information related to the threats to port security, the following general categories were applied:

1. Detection of threats,
2. Analysis and identification of security threats,
3. Dissemination of threat data, and
4. Ethical considerations in security operations.

For organizational development and dynamics, the principal subjects of interest covered were the following:

1. General organizational development
2. Interorganizational cooperation

The literature related to the study design has focused on the general philosophy of research, selection of a research worldview, determination of the most appropriate research approach and methodology choice that best suited the nature of the research environment, and the opportunities offered for discovering useful information. The reasoning behind these literature selections was that the subject of the present study involves a complex, public environment, in which multiple security threats potentially

operate and in which multiple organizations are needed to work cooperatively to meet and mitigate these threats.

Literature Search Strategy

The primary source of literature for this study has been the Walden Library, using the option of searching for articles by topic. The primary sources within that option have been the business and management section, and the policy, administration, and security section. Within these sections, some of the key words used pertained to security issues, such as *security, threat, law enforcement, risk, terrorism, vulnerability*, and other related words. In addition to these, key words used to find articles on organizational development included: *leadership, cooperation, coordination, collaboration, interagency, interorganization, jurisdiction,* and *ethics*. Principal databases searched were ABI/INFORM, SAGE Premier, and ProQuest Central.

In several cases, references from one article led to selection of additional articles if the additional references met the previously established criteria. Some of the selected articles also provided key words that informed further searches. In all of these cases, additional articles were selected exclusively from the Walden library database or linked sources.

All of these searches were conducted within selected restrictions to ensure that the articles would meet desired characteristics for the present purpose. These restrictions included articles published within 5 years of the original search, availability of full-text copies, and selection exclusively from peer-reviewed journals. Several of the referenced

books were found in my local public library or from my personal home library. In the latter case, most of the books were purchased in connection with previous Walden course work. In general, the books concern organizational dynamics or issues related to security and threat mitigation.

Conceptual Framework

Schein (2010) provided the general framework for the study in the form of a model of organizational culture development. This book was selected for two principal reasons: (a) it had already served as a text and reference book for previous Walden course work, and (b) it offered a description and justification for modeling organizational culture that fit the intention of the proposed research project. The conceptual framework, based on the three levels of culture and further described in the explanations of macrocultures, subcultures, and microcultures, established a set of observational models within which observations could be described and categorized. These models provided a standard set of descriptions for behaviors and events within the research environment, which served as a basis for comparison as well as a means of maintaining consistency in recording observations and interpreting results.

Another contribution of Schein's (2010) work was the description of the role of leadership and the exposition of various manners in which it may function within organizations. Leadership was seen to be a key factor both in establishing cultural norms and in gaining acceptance of them among members of cultural groups. Although sometimes difficult to directly observe, Schein asserted that leadership was detectable

through its effects on organizational functioning and the interaction of a group's members.

In addition to the Schein's (2010) models, the literature search also revealed research reports that, while conducted in different environments with different objectives from the study reported in this dissertation, nevertheless offered some methodological examples and corroboration of the Schein's models. For example, Solansky and Beck (2009) found that interorganizational cultures that developed shared acknowledgement of the importance of collaboration among organizations was associated with increased effectiveness and shortened response times in addressing threats. This shared acknowledgement or belief was seen to manifest itself in stated and professed commitment to collaboration. That commitment, as described in Solansky and Beck's paper, was consistent with the second level of culture, as described in Schein's book.

A negative but useful example of research that can be related to Schein (2010) was the Garrett (2010) study, which found that failures of large, interagency organizations to develop shared acknowledgement of the need for collaboration resulted in substantial inertia and general dysfunction in the larger organization. Garrett's descriptions of these problems were comparable to the understood, tacit sorts of belief (or lack thereof) described in the third cultural level described by Schein. The specific observations that led to the conclusion that this underlying assumption was lacking were consistent with the behavioral actions described in the first level of culture described by Schein.

In the Garrett (2010) case, the observed behaviors were seen to be both symptoms and results of the failure of organizational leadership to foster the kinds of cultural development necessary for effective functioning of interagency organizations. The leadership failures were examples of the type described theoretically in Schein's (2010) book. Finally, Chenoweth and Clarke (2010) found that existing organizational cultural norms, which were described in a manner that was consistent with the Schein's model, increased the likelihood that multilevel and multiagency organizations would coalesce successfully to make efficient use of available resources. In general, the current research collected for this study tended to indicate that the organizational culture models provided by Schein (2010) would serve effectively as a conceptual framework for the entire research project.

Literature Review

As stated in the introduction to this chapter, three domains of literature informed the plan for this study. Of these, the nature of the threat and means of countering it have been treated in the section entitled Types and Sources of Threats. Although some understanding of the security issues that comprise the work I observed was necessary for interpreting these observations, this domain did not directly influence the selection of a theoretical concept or methodological approach. Those choices informed by literature directly related to them. Thus, the following sections treat the subjects of research design and theoretical concept specifically, and the literature review was conducted with the

intention of identifying and subsequently justifying the selection of supporting organizational theories and methodological approach.

Types and Sources of Threats

Lutz, Roell, and Thiele (2013) delineated the types of threats that challenge security agencies in their efforts to maintain security of seaports. These threats, in general, fell into five types: (a) piracy and armed robbery, (b) maritime terrorism, (c) illicit trafficking, (including narcotics, weapons, human beings, and other contraband), (d) sabotage, and (e) cargo theft. Sources of these threats may be traditional and irregular warfare, terrorist organizations, and organized crime, in a constantly evolving and unpredictably interconnected mix. Lutz et al. (2013) further explained that the domain of maritime security encompasses more than just unimpeded conduct of maritime commerce, but also includes preservation of free access to the seas for all legitimate purposes as well as maintaining good governance of seaways to enhance operational safety and efficiency.

To provide this security, Lutz et al. (2013) prescribed a combination of both preventive and responsive measures, applied in a cooperative and systematic functioning environment. Cooperation and use of systematic protocols were identified as especially important because the means and causes of security threats generally cross jurisdictional boundaries. Attackers may travel by sea on their way to their intended points of action, or they may target port facilities specifically. Alternatively, they may attempt to use port facilities as bases of operation for attacks on ships at sea or inland targets, or they may

merely pose credible threats of any combination of these as a means of disrupting commerce or the general functioning of society.

Among the categories of action that required interorganizational cooperation, Lutz et al. (2103) named the following:

- inspecting vessels, terminals, and other facilities;
- responding to crises involving threats of terrorism or actual attacks;
- monitoring and controlling access to facilities and vessels;
- interviewing, examining, and credentialing transportation workers and facility personnel;
- conducting surveillance operations and participating in undercover assignments;
- tracking and interdicting suspicious cargo, persons, vessels, or vehicles;
- recognizing and detecting the presence of bombs, explosives, and weapons of mass destruction;
- interacting on security matters with vessel security officers, company security officers, facility security officers, and relevant federal, state, and local agencies; and
- performing threat, risk, and vulnerability assessments; security planning; and contingency planning.

Although Lutz et al. (2013) acknowledged that existing protocols were not yet adequate to accomplish these actions in a fully cooperative manner, they did observe that general agreements concerning the need for cooperation had been reached among many

nations and jurisdictions. This indicated that progress toward further cooperation may be expected. They did not, however, offer examples or descriptions of the ongoing efforts, nor did they identify specific areas of cooperation that remain to be addressed.

This lack was partially filled by Sandoz (2012), who also noted a lack of adequate cooperative protocols for maintaining security. In addition to the provision of active security measures among agencies, Sandoz (2012) indicated that general governance processes were needed. The absence of sound maritime governance was seen as a significant vulnerability that could be exploited by state or nonstate actors to disrupt, usurp, or block legitimate activities at sea and ashore. Sandoz (2012) concluded that individual jurisdictional entities such as nations or other political divisions should devise and announce their own protocols but should do so in consultation with other interested parties, including other nations. In this way, the entity responsible for maintaining and executing the policies and activities retains the right to determine what they are, while assuring other stakeholders that the policies will be compatible with the interests of all concerned.

Although useful and relevant to the present purpose, neither Lutz et al. (2013) nor Sandoz (2012) addressed the increasing dependence of transportation hubs on vulnerable electronic communication and data storage media. This more recent but significant issue regarding maritime security is cybersecurity. Kramek (2013) found that cybersecurity had received inadequate attention in most U.S. port facilities. According to this report, protecting data from unauthorized access, tampering, or destruction constituted a major

vulnerability, and although recognized as an issue, has not received the allocation of resources or higher authority needed to establish a program of strengthening defenses against cyberthreats.

Kramek (2013) asserted that port facilities rely as much on networked computer and control systems as they do on waterfront workers. Even so, the study found that no common standards for cybersecurity has been promulgated nor has authority over cybersecurity been granted to the agencies that are normally responsible for general port security, most notably, the U.S. Coast Guard. Furthermore, the study found that basic cybersecurity methods were not being practiced with sufficient diligence to prevent even relatively unsophisticated attacks. The consequences of failure to prevent major disruptions of computer and control systems would have an immediate and substantial effect on the U.S. economy by disrupting the flow of goods through the facilities, both for imports and exports.

To address these vulnerabilities, Kramek (2013) recommended several specific actions by Congress, various security authorities, and port operators. Some of these recommendations could be implemented immediately, while others would require many months and perhaps years to accomplish. Each increment of action on the issue was seen as contributing sufficiently to justify its implementation, even as others were still pending. Collectively, Kramek (2013) asserted that the recommended actions would greatly increase protections against cyberattacks while simultaneously producing disincentives for anyone who might attempt to commit them.

Threat Detection, Assessment, and Data Dissemination

Sims and Gerber (2005) provided a compendium of expert opinions that explored the field of security intelligence, counterintelligence, threat assessment/analysis, and communication of security data among cooperating agencies. From this comprehensive overview, it was evident that the critical issues involved in gathering and using security information are profoundly complex. Processes for gathering of information involve substantial degrees of vertical and horizontal communication because some entities with access to sources may not be aware of the need to exercise that access. Conversely, entities with clear understanding of threats may not know that some other cooperating entities have the ability to collect relevant data. According to Chalk and Rosenau (2004), this kind of difficulty is especially confounding for U.S. security entities because U.S. intelligence and law enforcement agencies are much more disparate and separated by jurisdictional boundaries than are their counterparts in other Western countries.

For these reasons, establishment of reliable means for sharing information among agencies is difficult but necessary. Agencies that report at the federal level tend to have the most extensive resources for collecting general threat data and for comparing large masses of data in a way that permits the extraction of meaningful conclusions. These agencies, however, are limited in several ways. First, they each have specialty areas in which they are required to operate. Generally, these specialty areas confine them to specific kinds of operations while excluding other agencies from directly participating in those operations.

Secondly, the allocation of resources limits all agencies, forcing them to prioritize their operations. These priorities may not be compatible with priorities of other agencies. Finally, the selection of specific activities must rely largely on the professional judgment of senior members of each organization. Regardless of the degree of professional competence, these judgments are dependent upon the quality of the information available to support them. Because all agencies must rely on at least some data from other agencies, thorough and efficient coordination is imperative (Garrett, 2010).

Even while members of most agencies recognize this necessity, there remain many structural and procedural impediments to full and efficient sharing of data. Chappell and Gibson (2009) investigated one of the most widespread of these impediments, in the case of community policing. Chappell and Gibson (2009) discovered that there was broad disagreement on the issue of compatibility of community policing and the centralized, federalized operation of homeland security operations. While some local police officials believed that community policing and homeland security processes were complementary, many others felt that the two approaches were in conflict, and that attempts to conduct both in the same environment were counterproductive.

In the specific case of the subject seaport, this issue was identified as one of the key factors of interest. This is because there has been a long-standing emphasis on community policing among some of the agencies involved, while there has also been a strong federal presence in some areas of the study environment. Focus on this existing condition provided a useful paradigm for the larger questions about cooperation among

multiple participating security agencies, all having disparate roles, cultures, and organizational procedures.

This phenomenon was further explored by Lisle (2013), who described the dynamics of breakdown of communication, and thus, cooperation, among stakeholders in the process of maintaining security. This issue was seen as being especially acute in cases where the actual nature of the activity to be protected had to be modified as part of the security provision. When this kind of issue arose, there was the potential for significant conflict between the protectors and those protected by them. Lisle's findings underscored the importance of examining and describing the dynamics of the many interactions that had to occur in threatened environments, in order to manage the interactions in a way that prevented misunderstandings and conflicts.

Giblin, Schafer, and Burruss (2009) found that there was an apparent causal relationship between perception of risk among security agency personnel and their willingness to undertake preparatory and preventative actions. Also, there was a causal relationship between the number of preparatory measures taken and the confidence of the individuals in their ability to cope with potentially harmful events. When combined with Lisle's (2013) findings about interactions among interested groups, and Giblin and colleagues' findings about factors affecting willingness to prepare, and confidence in the efficacy of preparations, there was useful guidance for inquiry into the current attitudes and expectations that may affect interagency coordination and cooperation in the current study.

Another potential difficulty concerned individual talents and capabilities that cannot be separated from specific job requirements. Johnson (2009) described some of the characteristics that are required for individuals conducting specific kinds of security related jobs. Some of the combinations of traits may prove to be rare, which require recruiters, managers, and administrators to accept compromises, in order to optimize, rather than maximize the desired characteristics of selected individuals. In such cases, there exists the potential for conflicts between these specially selected individuals and their peers in terms of internal relationships during normal, ongoing security operations. This dynamic adds to the complexity of maintaining effective coordination among operatives.

Dulles (2006) asserted that, while there are formal training facilities and programs for some types of security personnel, there are few, if any, that have proven to be universally appropriate for intelligence-gathering specialists. This is because the activities required for intelligence collection can be widely varied, and are generally more dependent on individual personality traits than on any specific skill set, "because [the operative's] abilities in the craft itself are more important than any specialized topical or area knowledge" (p. 174). This ambiguity is important, not only for the individual intelligence operative, but also for those with responsibility for selecting and assigning operatives. It constitutes another challenge in the general field of security work.

The issue of requisite skills is not confined to security personnel. Lack of skill and an attendant lack of adequate income are also seen as potential sources of security

problems. Belzer and Swan (2012) addressed this issue, describing the growing threat to the global supply chain, and, by extension, to the security of port facilities, that result from the growing use of low-paid, minimally-qualified, and inadequately screened and monitored transport workers. This kind of issue not only creates a special vulnerability for the transport industry, but also invokes the fundamental conflict between efficient and economical transportation activities and the kinds of security measures necessary to protect them from criminal and terrorist threats.

Belzer and Swan (2012) described the conflict as being one for which decision makers need to be aware that apparent expedients, especially those involving the minimization of costs such as payroll, may not always maintain an optimally efficient and profitable operation. Low-paid and low skilled personnel, who often have independent custody of transport containers, are found to be vulnerable to a variety of incentives and coercion from criminal or terrorist operatives. Visible cost savings may seem to be advisable from a profit-driven decision process. “In high risk-situations, however, widely dispersed compensation associated with market-driven pay may be associated with undesirable and inefficient outcomes” (Belzer & Swan, 2012, p. 41). The difficulty of coping with this reality is that the immediate cost is readily apparent to managers and their accountants, while the risk cost is both uncertain and difficult to quantify. Because of this difficulty, the burden placed upon security agencies is increased, due to the unwillingness of transportation managers to expend the resources necessary to mitigate some risk factors at the source. This fact tends to increase the opportunity for threats to

be introduced at the departure end of the transportation chain, which increases the likelihood that threats will be undetected at the receiving end. For purposes of the subject of this report, this factor was deemed to be potentially significant for the study participants and the security duties they were expected to perform.

International Cooperation

Nau (1995) argued that strategic security policy requires extensive international cooperation, and must involve such issues as trade practices, as well as intelligence and mutual security enforcement activities. This kind of necessity further complicates the task of security agency coordination, because it involves political policies that may often be at odds with the most expedient and reliable security processes. Nevertheless, the need for inclusion of trade issues in the complex equations of security cannot be ignored. This is not only true because of the need to maintain international trust and cooperation, but also because many of the threats to security have for their main purpose the disruption of international trade. Thus, international negotiations for trade policy will often include negotiations regarding cooperation in the realm of mutual security. Although this is primarily a policy issue that is beyond the scope of the current purpose, it does add to the complexity of the task, and awareness of this factor may influence some of the interactions among local organizations that have differing international interfaces and differing priorities regarding accommodation of non-United States entities.

This is also a potential area of discussion for the kinds of issues examined by Belzer and Swan (2012). If individual shippers are found to be reluctant to take

mitigating steps, due to real or imagined competitive pressures, perhaps host countries may be convinced that it is in their best interest to impose broadly applied standards of employee training and screening. Until this is done, however, the risk remains focused largely on the destination environment and the security agencies responsible for it.

Elements of Tradecraft

The processes for gathering information are both driven and delimited by all of the above considerations. *Tradecraft,* or the techniques and methods of intelligence operations, is dependent upon many factors: (a) technology, (b) policy, (c) politics, (d) resources, and (e) externally-imposed conditions. All of these factors remain in play during the information gathering process, and must be understood and considered.

Technology of Tradecraft

The technology of tradecraft is arguably the most independent of the factors. As new technological capabilities become available, they may generally be evaluated and selected according to their potential for enhancing operations. For this factor, the primary consideration is availability of sufficient budgetary resources to acquire and deploy new technologies.

The actual use of technologies, even when such use is both feasible and desirable from a purely operational point of view, may be, and often is, restricted by policy. For many reasons, security policy may limit the use, or even the acquisition of new technological capabilities. At the organizational level, policy is the immediate control element related to the technology of tradecraft. Policies may be influenced by such

factors as interagency jurisdictional boundaries, a desire to avoid redundancy or excessive dependence on particular technologies, or perhaps even the philosophical preferences of policy makers. Most often, though, policy is driven by politics.

Tradecraft Policy, Politics, and Resources

Dulles (2006) described some of the complexities of disseminating intelligence data and analysis to the policymaking authorities that need it to support security decisions. Timeliness and accuracy are, of course, of paramount importance, but there is also a multitude of other considerations. Some considerations relate to the analysis itself, such as the juxtaposition of timeliness and accuracy.

In order to be useful to the consumers of intelligence, it must be interpreted in a way that it can be related to the policy decisions that may be influenced by it. The interpretations must provide relevant data in a form that can be understood by policy-makers who may not be able to comprehend it in an unrefined form. Such processing of data necessarily takes time. The task of the intelligence team becomes one of determining a deadline for delivering the information in time to be useful, while allowing sufficient time to ensure the accuracy and comprehensibility of the intelligence report.

Johnson (2009) provided explanations of relationships between policy, and the means of executing policies. In general, policy provides the governing guidance that defines the goals and intentions of the intelligence work. As such, it becomes the task of practitioners to establish strategic frameworks through which the policies are to be carried out, and to implement tactics that will actually accomplish the work.

Throughout the entire process of intelligence gathering, analyses, and dissemination, there are guiding values that must be honored. In essence, the values constitute the ethical framework of intelligence tradecraft. Failure to adhere to the ethical values can have many negative effects (Olson, 2006). Even when common values are shared and upheld among multiple agencies, there can still be conflicts, due to differences in specific agency interpretations, or the effects of higher-level authorities of various jurisdictions imposing specific rules and procedures.

External Influences on Tradecraft

Much of the intelligence activity must necessarily take place outside the United States. This requirement imposes a variety of restrictions on both the nature of the activities used to gather intelligence, and the quality of the resultant information. For example, it may be difficult, due to host country restrictions, to establish independent sources of information that do not have to pass their reports through some official government source.

In addition, it may be difficult to accurately assess the real value of an information source, as in a case cited by Johnson (2009) in which a volunteer source, who seemed to be well placed, was eventually found to be completely unreliable. Initially trusted, the source was later recognized as more hindrance than help, whose information was either irrelevant or deemed to be false. Although developing corroborative sources can help to avoid this kind of difficulty, such sources can often be impossible to identify, or dangerous to employ. Another external dynamic that can negatively influence the

effectiveness of intelligence work, is the kind of incompatible norms of participating agencies that have formed one of the issues for this study. Although outside the scope of the present work, the findings from the current study may eventually prove to be of some use to practitioners who must cope with interagency issues in external environments.

Ethical Considerations

Domestic factors, too, may influence the practice of tradecraft. Some potentially valuable sources of information may have conflicts with ethical practices in their own professional fields. For example, the use of journalists as information sources, even in critical situations, can have severely negative results. For this reason, intelligence gathering activities enlist the cooperation of individuals outside the security community must be done judiciously (Olson, 2006).

The level at which tradecraft is practiced may also have an influence on the manner of its execution. The very existence of multiple levels of operation may generate decisions that would not have been made in isolation, particularly in situations where various rules of behavior conflict. For example, U.S. federal activism on security issues within local or regional jurisdictions may motivate the lower level officials to enact policy decisions that are designed to prevent what they feel is federal interference in their domains.

Woods and Bowman (2011) observed this phenomenon at various levels, especially when multiple regional authorities perceived federal intrusion. It was not only extant federal actions, but also those that were anticipated that were seen to motivate state

behavior. This was a source of mistrust and friction between municipal authorities and those above them in the hierarchy.

Organizational Theory

As stated earlier, Schein (2010) provided the principal guidance for building a theoretical framework for the study. Within the constructs offered by Schein, the proposed research will involve conducting interviews and observations in a manner consistent with the models previously described. The models employ reliance on existing researcher knowledge of the subject and research environment, and consist of face-to-face interviews that are guided by a standard interview questionnaire and format. These interviews were augmented by observations of ongoing security related activity in the research environment. In this way, consistency of the data collection processes has been enhanced, and the framework provided a convenient means of organizing the information as it was collected. The use of these models has also helped systematize the organization of the body of data, so that crosschecking and cross-referencing of participant responses and researcher observations was easily accomplished. This, in turn, helped to strengthen the credibility and dependability of the data.

The applicability of the theoretical models to the present purpose has been supported by use of current research works, which have either employed or observed the principles provided by Schein (2010). The reports by Solansky and Beck (2009), Garrett (2010), and Chenoweth and Clarke (2010) each provided useful corroboration for the Schein models, in a context that was found to be applicable to this study. With the

theoretical models thus supported by current research, Schein's model has proved to be a sound foundation for conduct of the project.

Guidance for Research Design and Execution

Despite the large body of literature available about a variety of security topics, my search for specific data about the transition from collegial, ad hoc cooperation among members of agencies, to a more formalized, top down structure for interface protocols has yielded little useful information. In fact, there are indications that some researchers, such as Eriksson and Rhinard (2009), as previously noted, have concluded that much more investigation is needed to determine the state of such transitions and the problems associated with trying to accomplish them. This tends to corroborate my early impression, gained from preliminary study of the research environment, that the nature of the process of transition and its inherent risks and difficulties are not well understood.

As a guide for selection of a research approach and methodological design, this lack of understanding favored a qualitative approach, using a case study methodology. This type of reasoning was provided by Trochim (2001), who asserted that a qualitative study may help not only to gain insights into the nature of the environment and phenomena of interest, but also to help develop new conceptualizations of issues that have not previously been proposed. "This is where most of the more interesting and valuable new theories and hypotheses originate" (Trochim, 2001, p. 152).

Martella, Nelson, and Marchand (1999) recommended that case study research be used when issues and phenomena of interest cannot be practically defined in advance.

Case study research was seen to allow the researcher to explore the research environment and research subjects, in order to identify issues and phenomena, and to modify the specific focus of the study while it was in progress. By such processes, the researcher could gain additional insights into research participants, and the environments in which they operated, in greater depth than originally anticipated.

With the foregoing indications favoring a case study, it followed that an appropriate case study design should be accomplished. This required consideration of the general nature of the study environment, identity and capabilities of the researcher, boundaries of the study, including geographical, organizational, personal, and temporal limitations, and availability of background information that could be used in preparation of the design, as well as evaluation of the findings. The principal source of guidance for the design was Yin's (2009) study.

Yin (2009) described the case study process as, "a linear but iterative process" (p. 4). Appropriate for a study in which an in depth and detailed description of a phenomenon (or phenomena) is desired, a case study was prescribed for explaining the how and why questions regarding the topic(s) of interest. Instructions for designing a case study began with the process of defining the units of analysis, followed by explanations of the general theoretical orientation of the study, and the propositions or issues to be studied. These descriptions would then inform decisions about the procedures to be followed, the questions to be addressed, the limits of the study, and the role of the observer.

Yin (2009) also suggested using the design criteria to establish the metrics for measuring quality of the findings and conclusions, and for establishing the case study protocol. To comply with this suggestion, the design criteria that govern acquisition of information about participant perceptions have also been applied to the establishment of success criteria. That is, if the interviews yield sufficient data to provide for a comparison of official guidance with actual practice, that portion of the study may be considered successful. Likewise, if observations of activities in the research environment yield sufficient data to make meaningful comparisons of observed activities to official doctrine, this too may be considered a successful outcome.

Further guidance for developing the study was provided by Stake (1995). Some of this guidance related to the interpretive nature of case study research. Interpretation, according to Stake, should be part of the planning process, because some interpretation necessarily occurs during the course of the study, while other interpretation is done after observations and other data gathering activities have been completed.

As with the quality metric process discussed above, interpretations have also been accommodated, in the sense that allowance has been made in the research design for before-and-after interpretations of phenomena in the research environment to be compared. In this way, interpretations themselves will have been subjected to internal quality checks. If a pre study interpretation of some phenomenon was found to be substantially different from its post-study counterpart, the assumptions that led to study elements, such as interview questions, may be reviewed for possible reinterpretation. This

process has also been accommodated for observations of activities and examination of official documentation.

Summary and Conclusions

As expected, the body of literature available provided background, guidance, and indications of need for the present study. The subject of security threats has received considerable attention, including descriptions of the nature and types of threats, means of combating the threats, and the implications of conducting security operations in a dynamic commercial and social environment. Organizational dynamics has been the subject of extensive study for generations, and the literature has continued to be reexamined and updated, so that the main task in planning the current study was to select the most suitable publications from the large body of available data. Likewise, research design has drawn the attention of numerous professional researchers who have written extensively on the subject. As with organizational dynamics, the main task has been to apply the recommendations that promised to be most appropriate for the present purpose. Chapter 3 includes a detailed description of the research methodology.

Chapter 3: Research Method

This chapter begins with a description of the selected research methodology, and an explanation for making this selection, rather than some other method. This is followed by a description of the role of the researcher, detailed description of research procedures and research questions to be addressed. Finally, the chapter contains information about various issues related to trustworthiness in the research, including procedures to enhance trustworthiness. The chapter concludes with a summary.

Research Design and Rationale

The decision as to whether to use a quantitative or qualitative approach was relatively unequivocal. Trochim (2001) described the conditions and procedures required to conduct a quantitative study, whether observational or experimental. Both conditions required that the research environment and research questions were permissive of sufficient bounding of variables and collection of exclusive data to yield results that could be analyzed quantitatively. These conditions could not be met in the research environment, because sufficient controls on data generation could not be maintained. This same limitation also prevented the use of the quantitative measurement necessary to satisfy the requirements of a mixed method study, thus neither quantitative nor mixed methods was selected.

Conversely, observational opportunities for identifying activities and relating them to individual participants and groups were established. This met the general set of

conditions necessary for a qualitative study (Trochim, 2001). With this determination, it was necessary to select the most appropriate design for a qualitative study.

One of the candidate designs considered was ethnography. While perhaps feasible, in terms of observational opportunities, ethnographic studies require the researcher to develop descriptions of a particular culture within the research environment. In fact, multiple cultures were considered likely to be in operation, but were not relevant to the purpose of the research. The same could be said of phenomenology. While perhaps interesting, specific perceptions of participants would be difficult and time-consuming to determine, and would probably not yield data about the operational relationships among participants in their professional activities.

Grounded theory offered some promise, and was considered. In this type of design, it would have been necessary to develop a theoretical explanation of the observed behavior of participants. This theory would then have been iteratively modified through further observation. The negative factor involved in this type of approach was that the theory itself would have necessitated certain limits on the observational process. Because the research opportunity available for this study was to interview and observe, in order to derive conclusions, and not to gather data for theory formation, grounded theory was rejected.

Given that the purpose of this study was to observe, inquire, and examine the activities of security agency personnel, and to discover factors that are associated with collaboration within the study environment, a research design that facilitated those

pursuits was determined to be needed. Considering the characteristics of the research environment, the focus of the research, and the open-ended nature of the issues that were explored, a case study methodology emerged as the most appropriate. This determination was reinforced by Creswell (2007), who advocated use of case study methodology for studies to be conducted within bounded systems, such as a specific setting or context. Further support for the selection was provided by Yin (2009). The complexities of the interactions and interventions were greater than could be reasonably explored through use of other methods, such as surveys or experiments, and a key intention was to describe and illustrate the phenomena of interest (Yin, 2009).

This type of design has also been reinforced in that it allowed for my chosen role as observer-interviewer. Having worked in the research environment in the past, in a variety of assignments, I have sufficient understanding of the environment to allow for thorough identification and examination of all relevant areas of the environment. The dynamic nature of the research environment also favored a case study, due to the increasing complexity and volume of operations in the port. The increasing number and variety of criminal and terrorist adversaries continue to exercise ever-greater ingenuity in finding ways to defeat existing security measures. At the same time, the various agencies holding jurisdiction over multiple aspects of port security continue to evolve, as threats, political pressures, and opportunities for growth and improvement increase. These characteristics complicated the process of preplanning, and required that the research

process have sufficient flexibility to allow for modifications that result from interpretation of some data as it is revealed.

One of the key strengths of case study research is that it allows for this concurrent data collection and interpretation (Stake, 1995). Creswell (2009) offered a similar justification for a case study, in describing the task as being intensively focused on an individual or context: "A *case study* is an intensive study of a specific individual or specific context" (p. 161). Given the dynamic nature of the research environment, and the fact that the intention was to intensively study that environment (context), a case study emerged as the most appropriate choice.

Role of the Researcher

My role as researcher was as an observer interviewer. My knowledge of the research environment derived from past experience in the environment, as a customer of some of the facilities therein. Although my past role has not been directly involved with security, I am familiar with the general issues and processes for maintaining it.

In addition, having worked in the environment, and with some of the participants, I have been able to gain the trust of those and others to whom I have been referred. My former role in the environment affords me some credibility with the participants, and I assured them that their identities would be held in strictest confidence. Through these assurances, and through the recommendations of selected acquaintances, I was able to recruit the participants needed for the study.

Even though my former work has not involved security, the fact of having witnessed, and occasionally participated in activities required by security concerns, should be recognized as a potential source of bias. To alleviate this, I have structured the questions, and the mode of displaying responses, so that readers of my report will have the information necessary to make their own interpretations, and to compare my interpretations with their own. This, of course, does not necessarily eliminate potential bias in selection of questions, or decisions to follow up on responses, but, by thoroughly describing the process, as executed, I believe that any bias may be either discounted, or allowed for by other assessors of my results.

Another check on potential bias is the offer by one individual to serve as an informal peer reviewer. This individual, who is thoroughly familiar with the research environment, as well as the issues under study, has reviewed my data, as well as my conclusions, to offer observations that may weaken my findings. Through this review I believe that my findings have been strengthened, by identifying and eliminating any fallacies. Because my interest is merely exposition of organizational development issues, with a goal of offering information that may help in the continuing development of a complex and dynamic organization, in which I am not a current or intended participant, I do not believe any meaningful conflict of interests have been created by this study.

Methodology

This has been a case study, focusing primarily on members of various organizations with responsibility for security in and around the subject seaport. Most data

have been collected through interviews, combined with observations of activities of some of the participants in the routine course of their work, which were augmented with examination of relevant, public domain documents that contained information about officially-promulgated policies and procedures to be followed by the subject organizations. In general, the procedures and techniques proposed by Stake (1995) have served as the guide for conducting the study, with additional guidance taken from Creswell (2007) and Yin (2009).

As suggested in these and other references, it was expected that the initial study plan would undergo modification during the course of the study, as new information, and perhaps additional participants were identified. This, in fact, proved to be the case, in that saturation of significant data obviated the need to interview the entire group of participants in the original plan. Descriptions, analyses, and conclusions are qualitative in nature, except that some quantitative analyses of groups of qualitative data proved to be substantive. For this reason, appropriate quantitative analytical techniques were employed. Although quantitative data inclusion was not directly anticipated in planning this study, the flexibility of the case study methodology permitted the use of quantitative analytical techniques, the results of which have been discussed in Chapter 4.

Participant Selection

As recommended by Creswell (2007), a purposeful sample strategy was used, selecting participants from a total population of approximately 400 individuals. Working from organization rosters, individuals were assigned sequential numbers, and participants

were selected on a random basis. This was accomplished by using a random number table to select sequence numbers, with the participants selected according to the random selection of their preassigned sequence number. The number of total participants from each organization was determined by the ratio of total number of members in the organization, relative to the numbers of members in other participating organizations. In this way, the purposeful nature of the sample was maintained, because each organization had at least some members selected for participation. Thus, the sample was held to a manageable size, while still providing a selected cross section of the total population. This allowed for in depth interviews, which yielded the desired level of relevance and detail (Yin, 2009).

Finally, although the possibility that some additional participants may be needed to help provide background information related to official documentation or other data related to the context of the research environment, this allowance in process proved to be unnecessary. All desired data was obtained through the planned interview and observation processes.

As indicated above, the intention was to include some participants from each of the large organizational groups. Essentially, this included law enforcement organizations from federal, state, and local authorities, military organizations with regular participation in some aspect of port security, and security personnel from nongovernmental (commercial) entities. This type of division yielded an allocation (out of 20 participants total) of four federal law enforcement personnel, two state personnel, ten local, two

military, and two commercial. It was considered possible that during the progress of the interviews, the resultant data might reach a point of saturation, with the preponderance of responses converging on similar views by the participants. This proved to be the case, which resulted in a reduction of interviews from the planned total of twenty, to the lesser number of seventeen. Even so, the planned allocation was sufficient to preserve the purposeful nature of the sample, while permitting random selection within the total population. It also allocated interviews to approximately 5% of the population of each agency, including U.S. Coast Guard personnel, U.S. Department of Justice officers, U.S. Department of Homeland Security personnel, State Police, Port Police, City Police, U.S. Navy, and local commercial transportation or warehousing personnel.

Instrumentation

The principal data collection instrument was an open-ended interview guide, using the interview questions listed in the Appendix. I developed the instrument in accordance with guidance provided by Creswell (2007) and Yin (2009). Other collection instruments were allowed for in the study plan, but proved to be unnecessary. The single exception consisted of my notes based on interviews, observations, general impressions of the research environment, and studies of published public data sources, to be used as explanatory or augmentative information related to observed activity in the research environment. As explained by Creswell (2007), interviewer experience with both the subject matter of the interview and the process of interviewing can have a profound effect

on the quality of the outcome, and in this instance, my previous experience with the research environment proved to be helpful.

Because the official documentation anticipated for use will be selected on the basis of its relevance to issues being studied, its accuracy is verified by definition. The principal interview instrument, and the questions contained within it, has been drawn directly from the research questions, which are at the core of this study. For this reason, it seemed reasonable to assert that the instrument is both appropriate and sufficient for the purpose.

Interview Questions. The questionnaire is presented in Appendix A. The research questions, and the related questionnaire questions, are:

RQ1: What security-related working relationships exist among all observable entities within the research environment?

- What is the role of your organization in the Port?
- How does your organization share security responsibility with other organizations?
- What other organizations do you interface with?
- How are decisions regarding security operations made between your organization and others?

RQ2: How have informal working relationships formed and what factors keep them functioning?

- What kinds of informal working relationships have you formed with members of your own organization?
- How did these relationships develop?
- What kinds of informal working relationships do you have with members of other organizations?
- How did these relationships develop?
- Tell me about any problems between the informal working relationships and the official direction that governs your work.

RQ3: What kinds of security threats are recognized within the research environment and how are they identified and assigned for action?

- Describe the security threats you know about that could affect the port.
- Among these, which ones are you involved in mitigating?
- How is your involvement defined and assigned to you?
- How secure do you feel in your working environment?
- What factors contribute to your personal feelings about security?
- What, if any, security threats do you think should be added to your assigned duties?
- If there are additional threats, why should you be involved with them, and what would be your role in mitigating them?

The last two questions were informed by Giblin and colleagues' (2009) and Lisle's (2013) studies, which helped define the need for information about factors that

influence perceptions of the quality of cooperative activities and the sources of confidence in collective preparations and preventative actions. With these general types of questions in mind, any responses that seem to indicate anomalies, difficulties, or conflicts between operational realities and official policy lead to follow up questions to further explore the issues.

Procedures for Pilot Study

The pilot study consisted primarily of preliminary interviews with key participants, augmented by review of related official documentation. Two participants were chosen for this purpose. This served to ensure that the study was feasible, based on access to the research environment and participants, and on the expectation that observable activities would occur with sufficient frequency during the course of the study, to enable adequate observation and data collection. To some extent, some elements of the pilot study were previously completed, in the process of gaining access to introductory information, such as that provided in the infrastructure liaison officer-training course. Preliminary discussions, but not interviews, were conducted, as part of the feasibility determination.

To further ensure appropriateness of interview questions, three preliminary interviews were conducted. These interviews were used to determine that the questions are understandable, and were conducted with participants who were not included in the main study. The outcome of this preliminary trial was that the questions were easily comprehended, and that they were appropriate for the purpose.

Participant Recruitment

Most of the participants were members of agencies holding responsibility for some aspect of port security. Some additional participants were also representatives of port user organizations, such as shipping companies, warehouse operators, or other waterfront businesses. Some of the participants contacted initially were management level personnel in the organizations of interest. Officers of the U.S. Coast Guard who hold management positions, such as members of the intelligence unit for the port, represent one such category of participant. Also, senior officers in the various police agencies and other emergency response agencies were included in the initial contact list. Based on responses from these individuals, additional participants were identified, with particular attention focused on those personnel who had regular working interfaces with counterparts in other agencies, whether those interfaces are formally directed through official policy, or informally conducted, through unofficial understandings among colleagues. Some participants from commercial or private user organizations were also included. This category of participant served only as independent evaluators of the degree to which security officials' assessments of noninterference with normal operations were viewed to be accurate, and their responses were not included in the analysis of results.

It was also deemed desirable to include some security officials from commercial companies. Two such individuals were interviewed, and their responses were included in the analyses, because, as security personnel, their responses were considered to be relevant in the same way as the members of government agencies. Finally, there were

some interviews with personnel from peripheral areas, such as the neighboring port that utilizes some of the common waterways and land approaches. These participants were recruited primarily from emergency response organizations that have regular interaction with counterparts in the study seaport. Because they were not regularly working within the research environment, their responses were not included in the analyses, but served as corroborative data.

To ensure ethical protection of the rights of all participants, no identification was made of any participants, even if some were willing to be identified or quoted. In this way, there was no possibility of inadvertent identification by omission. General descriptions of the types of participants were substituted for specific identities, and the coding scheme, described elsewhere in this document, was used to further ensure the anonymity of participants.

Although the characteristics of the ports made it difficult to mask their identities, even when names of the facilities are omitted, identities of individual organizations were omitted, wherever such omissions were feasible. Some organizational information, such as published, public domain policies, organization charts, and procedures, or minutes of open commission hearings, will necessarily identify their origins. Because these are already in the public domain, this should not pose an ethical issue, as long as no direct links are made between the published documents and individual participants who implement or comment on them.

Data Collection

This primarily consisted of interviews with participants, and observations of interactions among individuals from different agencies. Interview and observation data were augmented by document reviews, especially public domain documents related to interagency procedures and policies. Observation data consisted of researcher notes which listed and described observed activities, with particular attention to cooperative actions among members of different organizations.

Potential participants were identified through observations in the various work areas of the port, including piers, boatyards, cargo loading areas, warehouse areas, and ground transfer and shipping areas. Each participant was assigned a code number, known only to me.

Working from the random list of potential participants, initial contacts were made in the normal work area of each participant. At that time, the participant was told that the study was ongoing, and was requested to participate through an interview. If the participant agreed to the interview, an arrangement was made to meet at the participant's convenience, at a site that was mutually acceptable, and which offered sufficient privacy to avoid inadvertent disclosure of participants' responses.

At the outset of the interview meeting, the participant was briefed on the nature and purpose of the study, and was presented with the consent form, and asked to read and sign it. Prior to commencement of the interview, the participant was given the

opportunity to ask questions about the study, privacy issues, or other general questions about the nature and use of the data to be gathered.

A facilitating factor in this study is my former relationships with some of the participants and participant organizations, which helped to provide access and trust which might otherwise be difficult to attain. Preliminary conversations with some key individuals indicated that adequate access would be available. Likewise, preliminary review of public access documents has confirmed that sufficient documentary data was available to provide guidance related to official policy, and to serve as comparison baselines for analyzing the correspondence between officially sanctioned procedures and observed interactions. While not included for interpretation and analysis, the existence of the official policy guidance was confirmed through this process.

Interviews, while carefully planned as to content and mode of interaction, were conducted in an informal manner, as much as practicable. This was to encourage maximum openness from participants, and to draw out detailed information on the topics of interest.

Arrangements were made in the manner described above, to meet at a convenient location, preferably in or near the participant's usual work site. The interviews each lasted approximately one hour, unless follow up was needed. Only two such follow up interviews were required, and resulted from observations that indicated a need for specific explanation of the events observed. These follow up discussions were brief, and were conducted near the sites of the observations, by mutual consent.

In general, the topics of the questions corresponded to the fundamental questions addressed in the study, but with a greater level of detail. The actual questions were designed to elicit information about the research questions. Participants, especially those who took part in the earlier parts of the study, were encouraged to suggest further lines of inquiry, should they be aware of issues that were not covered in the planned questions. To help promote this type of voluntary additional discussion, each participant was briefed on the general purpose of the study, and the uses to which the results were to be employed. To help ensure that a reasonable sample of participant views would be gathered, it was intended that approximately 20 participants would be selected for these interviews. As the interview process proceeded, though, the unanimity of key responses created a condition of data saturation, so that the interview process was halted after a total of seventeen participants had responded.

The principal source of guidance for structuring the interview process has been Martella and colleagues' (1999) study. It provided guidance for all aspects of the process. Choice of participants, content of the interviews, mode of interaction, and formatting and sequencing of questions was in accordance with this guide. Familiarity with the study environment and the participants proved to be a significant factor. My own experience in the environment, combined with some of the organizations involved (although not in a security related capacity), has been a factor in my selection of the nature of the study topic and the study design. This fact tended to enhance my credibility, as well as the

degree of trust I enjoyed from participants, which seemed to positively influence their willingness to speak openly.

As mentioned above, participants received a general briefing on the study and its purposes at the time that interviews were scheduled. At the start of the actual interviews, a more detailed briefing was provided, including a description of the study objectives and general questions to be addressed. The objective was to gain information about actual inter-agency cooperation, and the manner in which the cooperation has come into being. For this reason, the open format of the interviews did not appear to materially affect the outcome, and seemed to elicit responses that originated with the participant, rather than being previously anticipated by the researcher.

Data Analysis

Data coding for analysis consisted of open and axial coding, in the manner described by Strauss and Corbin (1990). The open coding identified and developed concepts associated with properties and dimensions of raw data collected through interviews and observations of ongoing activities of personnel in the research environment. Through this process, data points could be examined for similarities and differences, to establish categories into which data items were grouped. These categories were then analyzed for use in the second coding process, which is axial coding.

Axial coding consisted of examining the categories from the open coding process, to find connections among them, in terms of context, conditions, actions and interactions, and consequences. This facilitated establishing relationships among the categories of

data, to infer causal factors, describe common or contrasting properties of the categories, and to describe actions that are taken by participants in their efforts to address the conditions and phenomena. Although Strauss and Corbin (1990) described techniques for achieving a grounded theory research design, and their techniques included more than just open and axial coding, those two techniques proved to be sufficient for the present purpose. This analysis helped yield indications of the outcomes and consequences of the actions, which, in turn supported the ultimate analysis of the data, in relation to the research questions.

With 17 participants each answering 20 questions, and each question yielding multiple data points from each participant, there was as a result, a very large number of data points. Because the amount of data is was sufficiently large to make manual manipulations of the data, as described above, difficult and time consuming, I employed a qualitative data analysis software package, to help organize and categorize the data. This not only reduced the time required to complete the analysis, but also helped identify categories and conclusions that might have been missed through manual examination, alone.

Document review. As a means of comparing official policy with observed operations, available policy and procedure documents were examined. Because most of the participants were members of public organizations, sufficient documentary information was available to enable an adequate examination of official guidance for

interaction of the security organizations under study. These documents are in the public domain, and most, if not all, are available online.

Other sources of general official guidance were also made available, such as the infrastructure liaison officer course materials. These materials outlined general processes for identifying potential threats, and for communicating resultant data among agencies, and between official agencies and nongovernmental entities with an interest in mitigating security threats. Various public-access meetings, documents, and special events have also proved to be valuable sources of general data about issues and preferred modes of interaction among interested entities. Review of this kind of data has helped inform the process of developing interview topics and questions.

During the planning process for this study, it was anticipated that there would be enough publicly available documents to support the research project, and this proved to be the case. Two principal areas of interest were associated with these documents. The first concerned participant compliance with, and attitudes toward the documents. The second concerned the degree to which official guidance was consistent between agencies. Although discontinuities or conflicting guidance would constitute a significant finding, none were found among local agencies. Some discontinuities were alluded to in the interviews, but these were between local agencies and those operating from outside the research environment. These offered some indication of opportunities for useful further study, but were considered to be beyond the scope of the current effort.

Observations of activities. Observations of operational activities focused primarily on those activities that required interaction among agencies, or which involved responses to emergent situations that may generate the need for interaction. During the observational process, the researcher watched people working in the research environment, and made notes of the observed activities. The principal factor of interest in these observations was the manner in which the interactions came about. For example, one specific factor was the apparent automatic assumption of tasks by various group members, or the lack of automatic assumption. If negotiation on the site was observed, this was taken as an indication that there may have been some gap in the interaction protocol, and follow-up interviews would probably have been indicated. The observations were recorded in the form of notes taken by the researcher at the time the observations are made. These notes constituted the observational data used in the interpretation process. During the course of the study, no such negotiations were observed, which indicated that either formal or informal protocols were already in place.

Whatever the nature of the activities, some follow-up was nevertheless conducted, to help interpret the observations. Even in cases where all participants seemed to interact in a habitual, predetermined manner, it was found to be useful to ascertain the origin of the apparent interactive protocol. As with interviews, observations of ongoing activity in the research environment were coded sequentially and chronologically. The in-process preliminary evaluations were used for quality assessment purposes in a manner similar to that described above for interview data.

Although the intention was to perform observations in areas that are open to the public, there is the possibility of data emerging during the course of the study that could require observations in areas that are not available for unrestricted public access. Should it have become necessary or desirable to perform observations in areas where special permission was required for entry or observations, such permission was intended to be obtained in writing, and submitted to the Walden Institutional Review Board, approval number 10-24-14-0145037, for approval. This proved to be unnecessary, as sufficient data was obtained through observations in public access areas.

Triangulation. Several means of triangulation were employed to enhance the credibility of the data. Data triangulation was accomplished through the analysis process, by comparing responses of various participants, particularly those who worked in different organizations, or whose tasks differ from one another. In this way, anomalies could be detected and resolved through follow-up activities, or through other types of triangulation.

Methodological triangulation was accomplished primarily through comparison of data gathered through interviews, with data gathered through observation of activities. This was further augmented with data from published, official documentation. In this way, researcher observations were used to corroborate or question responses from individual participants who answered questions during interviews. Some additional triangulation was achieved through comparison of official documentation to interview responses and observed activities.

Issues of Trustworthiness

Trustworthiness was enhanced by the triangulation and cross agency comparisons, as well as the fact that my contact with the research participants was available to continue for as long as seemed useful for checking and rechecking observations. An associate who currently works in a peripheral role in the research environment also agreed to serve as an informal peer reviewer, to help ensure that any serious misinterpretations were identified. This peer consultation has already been completed, with suggestions and observations accommodated.

Houghton et al. (2013) provided a useful description of the qualities necessary to satisfy requirements for valid and reliable research, as well as techniques for maintaining these qualities during the course of planning, executing, and reporting the research project. Additionally, Houghton et al. (2013) offered descriptions of extra, desirable qualities and procedures that augment the value of research findings. Several of the recommendations from Houghton et al. (2013) have been included in the planning and execution of the research project.

Dependability

In general, both Houghton et al. (2013) and Yin (2009) described reliability (or dependability) in terms that could also be called repeatability. For this study, repeatability was maintained by thorough documentation of all activities, including the manner of selection research participants, the modes of interaction between the researcher and participants, the specific selection of documents reviewed, and the interpretations of these

documents in relation to the research environment. Finally, to the greatest extent practicable, the general conditions prevailing within the research environment was also described in detail. These conditions included the kinds of work or other activity observed, the presence or absence of specific threats during the observation period, and other potentially influential factors, such as ship movements, cargo transfers, large scale civilian recreational activities, or other factors that may have influenced the actions of the personnel being observed.

Confirmability

According to Creswell (2007), validation or confirmability, can be one of the most vulnerable factors in producing a credible case study, and, if not adequately addressed, may leave the research (and the researcher), open to criticism for producing work that does not justify its findings and conclusions. To prevent this, Yin (2009) recommended three, mutually reinforcing techniques: (a) use multiple sources of evidence, (b) establish chain of evidence, and (c) have key informants review draft case study report.

Without these techniques, the research may be subject to criticism that the work, "fails to develop a sufficiently operational set of measures and that 'subjective' judgments are used to collect the data" (Yin, 2009, p. 41). Houghton et al. (2013) reinforced this recommendation, by suggesting exercise of what they called *audit trail vigour* to permit readers of the research report to determine for themselves if they agree with the procedures and conclusions described by the producer of the research. These

kinds of validating activities can help support a claim of objectivity, even in cases where the researcher has a perspective that may make objectivity difficult to defend.

Credibility

For this type of study, one of the most significant threats to credibility is the potential for induced bias and inconsistency, as the study progresses (Yin, 2009). As the researcher becomes aware of the trend of responses among participants, it would be natural to anticipate the responses and to modify the form and content of questions asked. Any change in form or content between interviews would introduce researcher bias. This undesirable influence would thus render later responses noncomparable to earlier ones.

To combat this tendency, each successive interview was planned in the context of previous interviews, with contingency questions decided in advance. In this way, some potential for bias could be detected and mitigated during the planning process. Although imperfect, strict adherence to the process rigor prescribed by Houghton et al. (2013) was employed to minimize the negative effect of researcher bias.

Further mitigation of bias was accomplished by use of the chronological and sequential assessment codes described above. Identification of progressive trends in responses was expected to reveal the possible influence of bias, which could then be subjected to further analysis, and, if warranted, modification. One further measure that can help maintain credibility is for the researcher to perform a thorough self assessment of personal expectations, values, and relevant experiences that influence selection of questions, participants, and issues to be explored (Diefenbach, 2009). The suggested

process involved introspective examination of personal reasons for selecting the specific factors to be researched, with the intention of identifying and explaining the selections. According to Diefenbach (2009), this technique can help enhance credibility, and can also be useful for other readers of the research report in conducting their own evaluations of the objectivity of the research. With this self-assessment in place, each successive set of interviews, observations, and interpretations can be compared to the assessment, as a means of establishing a personal baseline. This is, of course, at least as subjective as any other method, but once established, became another consistent measure of validity.

Application of these techniques seemed to be of benefit, and the results of the interviews did not indicate any excessive researcher bias. This belief was reinforced by the fact that both the manual and software analyses of the interview data indicated significant stylistic, linguistic, and content variability on the parts of the participants.

Transferability

For purposes of this study, transferability relates to the degree to which the findings and conclusions may be applicable to transportation hubs other than the one in which this study has been conducted (Singleton & Straits, 2010). Although generalization of the findings cannot be automatically assumed, some generalizations have been accepted as implicit in preparation for the study. The first of these implicit generalizations is the fact that all transportation hubs should expect to face similar types and sources of security threats.

To help establish transferability, and to enhance the general usefulness of the findings, thorough description of the research environment, exposition of its unique characteristics, and explanation of the complexities of interagency policies and jurisdictions has been included in the research report. The procedures to protect dependability, such as maintaining a rigorous and thorough evidentiary audit trail, and utilizing review assistance from outside observers, have also helped support an assertion of transferability. A final note on transferability is to avoid attempting to excessively generalize the findings, or to form a generalizable theory. This avoidance, described by Diefenbach (2009), can help maintain credibility of the study and its conclusions, by acknowledging the fact that the study was based on the activities of one researcher, working from a personal perspective, with realistically limited objectives, other potential users of the study can make their own assessments of its potential application to their own work or further research of the subject.

Ethical Considerations

The entire data collection process has been designed to scrupulously avoid ethical issues, especially those related to protection of privacy rights of individuals. The coding process, the aggregation of data in a manner that avoids individual attribution, and identification of type of work, rather than specific organizational membership of participants, all were designed to prevent inadvertent identification of participants. Description of these safeguards was included in the participant briefing, which did seem to further increase the willingness of participants to speak frankly about experiences and

issues, related to collaboration among members of their own organizations, and in multiple-agency activities. Willingness to speak frankly was also enhanced by the fact that participants were presented with a copy of the informed consent form, which was explained to them before they signed the form.

Summary

The nature of the research environment, combined with the availability of participants has served to make a case study both desirable and feasible. The growing interest in data that can support improvements in the effectiveness and efficiency of security operations at transportation hubs has given this study substantial current relevance, and the access to the participants and research environment that has been provided ensures that a meaningful addition to the body of information about the subject has been achieved.

The research plan has been based primarily on interviews with participants, in an open ended format, which was intended to explore, and then describe the dynamics of interaction among the many agencies that share responsibility for security at the seaport. Observations of several types of interactions were added to the plan, to provide continuity among the various inputs from participant interviews, as well as corroboration and independent evaluation of the interactions described in those interviews. A substantial number of official documents, which describe the policies and procedures that top-level administrators have prescribed for the interactions have also been identified and studied.

This has allowed for further comparison between official intentions, perceptions and expectations of operational personnel, and observable activities related to those intentions and perceptions. Together, these elements have coalesced into a research project that provided a confident expectation that the findings and conclusions are meaningful, with the potential for supporting further refinement of interactive effectiveness among agencies at the port, and perhaps at other facilities with similar needs and mandates.

The following chapters include descriptions and discussions of the outcome of the research. Chapter 4 includes details of the results of the work, while Chapter 5 includes implications of the research. The final chapter also includes topics for further study of the issues.

Chapter 4: Results

The purpose of this work was to explore issues that can hamper efficiency of security agency operation and collaboration, and to identify actions that have enhanced collaboration. To do this, I used a case study design, with data collection being primarily through interviews, augmented by observations of participants' activities in the research site. The observations were of ongoing activities conducted as part of the normal course of business.

Participants were randomly chosen from various organizations that were chartered to provide security related services at the research site, and the observations were made at various locations, at various times of day. To accomplish this, I followed a consistent process of contacting potential participants, obtaining their agreement to participate, and conducting the interviews. Likewise, with observations, I followed a consistent protocol for duration and observation. This protocol involved observing each area studied for approximately 3 hours, regardless of location or time of day.

To encourage open and thorough responses to questions, I offered all participants my personal assurance that their identities would be held in strictest confidence, a promise reinforced by a written form. A copy of this form is provided in Appendix A. Additionally, I described to each participant the identification scheme, which assigned a code number in place of the participant's name. This code number was substituted for the names in all notes and analytical documents to further ensure confidentiality

To enhance dependability, I used a single set of interview questions with each participant. This set of questions is provided in Appendix B. In addition to aiding in consistency, its use may also contribute to the dependability of this study, should other researchers wish to attempt replication. Although more than 20 organizations have responsibility for some aspect of security at the port, participants were selected only from those agencies that maintain a permanent operating facility within the confines of the port. In this way, the sample was drawn from a population all of which worked in the research environment. The total population size was sufficiently small that a representative sample would be small enough to be manageable within the practical limits of the study design.

This chapter includes the demographic characteristics of the participants, to the extent that those characteristics were relevant to the purpose. It also includes a description and results of a brief pilot study. Finally, the chapter includes descriptions of the research environment, the data collection processes used, the methods of analyzing the data, evidence of trustworthiness, and a chapter summary.

Pilot Study

The pilot study was intended to ensure that the nature and purpose of the study was comprehensible to the kinds of individuals who participated in the main study. By this means, I was able to verify that the written privacy assurance that was provided to each participant was clearly understandable. As in the main research, I also informed participants of their rights and protections related to their participation.

Two individuals were chosen from the same population as the participant group, but who were not participants in the primary research project. The explanation of the nature and purpose of the project given in the pilot study was the same one used in the main interview process. Likewise, the same privacy document was explained and provided to each pilot study participant. After this introduction, the pilot study participants were asked to describe their understanding of the briefing content. Both pilot study participants were able to demonstrate clear understanding of the key points, as well as their rights and protections. As a result, the briefing and privacy document were determined to be appropriate to the purpose.

Setting

The research environment consisted of a large, multiuse seaport, with facilities for accommodating container and bulk cargo ships, as well as smaller vessels. Most of the facilities are on an island, surrounded by a narrow waterway that provides access to pier facilities. Pier facilities house numerous rail-mounted cranes, with provisions for immediate removal of offloaded cargo, and for staging of cargo to be loaded onto ships. There are also several hundred acres of accommodation for surface transportation of goods, including truck and rail transport facilities. Warehouse complexes and facilities for providing maintenance and repair of ships, boats, and ground transport vehicles augment these facilities.

In addition to the facilities that support large-scale cargo handling, there are also numerous recreational, marine research, and commercial facilities, such as pleasure boat

docks, retail businesses, and dining establishments. Finally, there are several facilities housing official, security-related organizations, as well as a medium security prison.

Waterways

The principal waterways consist of a single, main channel, which is approached via an outer harbor that is protected by a sea wall. Outside of the sea wall, in the open ocean, there are numerous designated anchorages for large ships awaiting clearance to enter the port. Smaller waterways, providing access to marinas and other facilities requiring waterborne approaches, are cut into the island from the main channel, or from the outer harbor.

Added Complexities

A major, added complexity, both operationally and organizationally, is the existence of another large seaport adjacent to the venue of this study. This port is under the jurisdiction of a different political structure from the study venue (a different city operates it) and has its own security agencies, several of which operate in parallel with those in the study venue. Furthermore, the two ports share several of the waterways, as well as the roads, bridges, and railways that serve the venue port. This nearby, and sometimes overlapping set of organizational jurisdictions, increases the criticality of ensuring that security operations are coordinated and cooperative. This feature was included in the current study, because it unavoidably affected some of the issues that arose during the data gathering phase. Even so, because the intention was to include only organizations that maintained permanent facilities within the confines of the study port,

no organizations from the adjacent port were included. The existence of this proximate facility did influence some of the recommendations for further study that have been included later in this report.

Figure 1. View of a section of the port, showing piers for ship mooring and cargo transfer.

Demographics

Study participants were all members of local organizations, and were expected to be familiar with the local environment. This condition was expected to give the participants a common focus on security related issues within the research environment. Other demographic data, such as ethnicity and gender, were not considered to be directly relevant to the study purpose, and were not recorded.

Categorization of Participants

Because cooperation among individuals and organizations was the primary focus of the study, the principal descriptor chosen for participants was the kind of work they did. This enabled a concentration on issues related to getting the tasks accomplished, within each of the general areas of specialization practiced by the individuals who took part in the research. It also enhanced the identification of differences among the various organizations in policies and procedures related to similar tasks.

Participants were characterized by one of three categories reflecting their primary functions: law enforcement, safety and rescue, regulatory enforcement. This categorization was maintained irrespective of the primary function of their home organizations, because some agencies have multiple roles in port security, and it was the nature of the individual participants' work that was of most interest (see Table 1).

Table 1

Number of Participants by Specialty and Home Agency Type

	Safety	Enforcement	Regulation
Law Enforcement Agency		4	1
Regulatory Enforcement Agency	1	2	2
Safety and Rescue Agency	2	1	2
Commercial Operator		2	

Note. Rows depict mission responsibilities of home organizations; columns depict number of participants by personal specialty or current assignment.

Data Collection

The data collection process consisted of a combination of interviews with participants who work in jobs related to maintenance of security within the port perimeter, observations of those kinds of personnel in their working environment, and study of official documents that pertain to the operation of security related agencies. The primary source of data was the interviews augmented by the observations. The document

search served to help provide context and understanding of the objectives and priorities of the agencies involved.

Interviews

Although the plan called for interviews with 20 participants, the results began to approach saturation after approximately 12 interviews had been completed. Results from an additional five interviews, which had already been arranged, did not materially affect the outcome. As a result, the final three interviews were not scheduled.

The interviews were conducted in locations in or near the research environment, and were chosen by the participant. The duration of the interviews averaged approximately ninety minutes, with some lasting only 1 hour, and others extending beyond 2 hours. I also did two follow-up interviews that resulted from observations of activities in the research environment. These follow-up interviews occurred at or near the sites of the observations, lasted only a few minutes each, and were specifically for the purpose of explaining the observed activities.

The results of the interviews were initially recorded as hand written notes taken during each interview, which were transcribed later, usually in the same day. During the transcription process, any data missing from the notes were filled in from interviewer memory. As expected, the participants who agreed to be interviewed showed little or no reluctance to answer the questions fully and openly. Before concluding each interview, I would explain my understanding of participant responses, to ensure that I was accurately characterizing the participant's meaning.

Observations

Seventeen observations were conducted within the boundaries of the research environment, that is, within the confines of the subject seaport. Each of the observations involved at least one member of an organization to which one of the participants belonged, although not all of the observed individuals were interview participants. They were conducted at random intervals, for a period of three to four hours each. Because four of the observations involved interactions between members of one or more of the organizations included in the study, and, as stated above, two of the observations stimulated follow up interviews.

To perform the observations, I positioned myself in a vantage point within the port from which I could watch activities over a wide area. In some cases this entailed watching ongoing work in an area where members of one or more of the organizations conducted their usual activities. In other instances, the areas under observation required only intermittent activity by any of the organizations of interest. For example, one area observed contained a dispatch station, from which organization members regularly emerged and proceeded to some other point where their presence was required. For some of these, I was able to follow the individuals, to watch what kinds of activities or interactions resulted.

In some other instances, I would merely watch a wide area that was under the jurisdiction of one of the organizations. When any activity occurred, I would make note of the nature of the activity, as well as any interactions between members of more than

one of the organizations of interest. If the purpose of the interactions were not clearly evident, I would follow up with in person questions, requesting explanation or clarification.

While necessarily random, I found these observations necessary to clarify information obtained through the interview process, and also to corroborate some of the information provided by participants. The random nature of the observations, combined with the fact that many kinds of activities do not occur at predictable times, resulted in limitations on the extent and detail of the data obtained. These limitations are explained in the section entitled Limitations, in Chapter 5.

Documents

Additionally, publicly available policy statements and directives, pertaining to operations of security agencies at the port, were also examined. Although useful, these documents did not yield any data that was included in the data analyses. They did; however, serve as background to assist me in comprehending observed activities.

Data Analysis

Three modes of data analysis were used for this study: general perusal of all recorded data by me, a manual comparison of interview responses to observations, and entry of all interview transcripts into NVivo 10 software, for detection and identification of major themes and commonalities in the interview responses. Each of these modes was useful in different ways. For example, the general perusal helped to verify consistency in data collection and collation. Comparison of observations to interview responses was

most useful in the fact that some previously unidentified activities yielded additional data that had not emerged from other modes of inquiry. Finally, the NVivo software helped me to accomplish the task of identifying themes that were evidenced by the frequency of appearance of specific subjects or ideas. This mode of analysis provided some of the most useful elements of data examination for inductive study of responses related to the research questions.

Identification of Categories and Themes

One of the expected themes that did not appear was a concentration of attention to, and awareness of the importance of cyber security. Because of the increasing incidence of this type of threat in many environments, it was anticipated, during the planning for this research, that most personnel in security related jobs would be aware, if not preoccupied, with this issue. This absence was noted during the general perusal of collected data. An example of the lack is evident in the following typical response regarding the types of threats to port security the participant was aware of. As participant identified as E-3 stated:

> We have to watch for everything. Terrorists, speeders, drug dealers, and a lot of drunks.
>
> We also get burglaries. There's a lot of valuable cargo that goes through here, and people try to steal it (participant E-3, personal communication, October 29, 2014).

Most of the responses to this question were similar to the one above. Although some of the responses were considerably more detailed than this example, only two mentioned cyber security, and those did not afford it any special significance.

Another unexpected absence was the lack of emphasis on use of the Fusion Center by participants. Only a small number of participants even mentioned the Fusion Center, although all seemed to be aware of its existence. Those who did mention it did not allude to it as having any special significance in their routine execution of their duties, except for occasional inputs of information. The one response that seemed to give the Fusion Center the greatest significance was from an individual, identified as participant E-5, whose principal work involved waterfront law enforcement.

> We work for the Chief, but I know he has to listen to a lot of people. The mayor, the [port executive director], even the [USCG] captain of the port. They all have a say in what we do and how we do it. I guess the feds get into it sometimes, especially if it's about drugs or terrorists. We also get calls from the [Fusion] Center. Sometimes it's something important. Mostly not (participant E-5, personal communication, November 5, 2014).

During planning for this study, I had expected the Fusion Center to be central to the operation and cooperation of agencies on the waterfront, because of the emphasis and major allocation of resources by DHS. According to the data collected for this study, the security operatives in this research environment did not consider it to be of major significance. I had also been unaware, during the planning phase of my study, that the

local Fusion Center was actually located within the boundaries of the neighboring port, and not within the research environment, as I had originally understood. For this reason, as well as the lack of importance expressed by participants, I omitted the Fusion Center from my list of observation sites.

One of the more positive themes that emerged from the NVivo analysis was the importance of trust. This recurring reference appeared in many of the transcripts, in various contexts, but always held special significance. For example, participant S-3, whose principal duties involve fire safety and rescue, responded to the question regarding informal vs. formal working relationships.

> We are all one team, but everyone knows who is best at certain jobs. We have specific, defined assignments, and we work according to the duties of those assignments. But there are always some kinds of work that we divide up among ourselves. I mean, we also have close friendships. You can't work in this kind of organization without knowing whom you can trust, and trust takes time to build up. That trust comes from people being dependable in formal relationships and informal relationships. (participant S-3, personal communication, November 1, 2014)

This is only one of the many contexts in the data where the concept of trust emerged. The NVivo analysis disclosed widespread significance of trust in a variety of contexts.

Two other significant themes emerged from the data, including the effects of jurisdictional issues that occur between organizations, and the influence of competition

for funding, especially from federal sources. There were numerous references to these issues. They will be discussed more fully in the section on Results.

The principal discrepant themes that have emerged from analysis of the data were the negative ones discussed above. Most other themes were consistent with objectives and expectations that guided the planning for the study. All of these have been discussed more fully in the Results section of Chapter 4 and in various parts of Chapter 5.

Evidence of Trustworthiness

The trustworthiness measures described in Chapter 3 have been followed throughout the process of planning and executing this study. The principal means of attaining trustworthiness has been the systematic process of data gathering, particularly in the conduct of interviews. Each interview was conducted using the same set of interview questions, in the same sequence. Although participants have been encouraged to embellish their responses, each response has been associated with a specific question, and all recorded responses have been made in the same sequence. Similarly, the observations have all been conducted in the same manner, with the only variations being time of day and specific location within the research environment. Strict observational protocol has been maintained throughout.

The standardization of the data gathering process, and the systematic execution, should allow for accurate replication by other researchers who might desire to make the attempt. Review of documentation was similarly systematic and replicable, because all documents selected were available to the public. The comparison of these sources of data

has provided a means of triangulation, and no major anomalies have emerged. These same techniques have contributed to credibility, by demonstrating consistency in both the data gathering process and in data analysis. Transferability has been made implicit, in that the types of organizations involved have been identified, and their relationships described. Given that other transportation hubs face similar threats, comparison and contrast can be done by examination of issues in the present research environment against those of other environments.

Dependability has been maintained through strict adherence to data gathering and data analysis protocols. Any other researcher should be able to replicate the study by following them. This is also true for confirmability, in that the kind of audit trail of evidence, as recommended by Houghton et al. (2013), has been provided through exposition of data and the methods employed to analyze it.

Results

The data gathering process has yielded answers to the research questions in a way that can be used to identify significant influencing factors, as well as providing bases for recommendations for future actions. While both formal and informal relationships among individuals and organizations were found to exist, there were some conflicts identified between official policy and practical execution of individual duties. The manner in which these conflicts have been routinely resolved may prove to be instructive, and the factors that enable individuals to confidently reconcile the conflicts should also prove useful.

RQ 1 and Related Themes

RQ1: What security-related working relationships existed among all observable entities within the research environment?

Theme 1: Command Media. All participants acknowledged that formal relationships were defined by some type of command media, depending on the type of organization the participant represented. Those elements of the relationships that related to general mission of the organizations, and the manner in which the individuals' duties were to be performed, were generally seen by the participants to be unequivocal and reasonable.

In some cases where formalized interagency cooperation replaced existing, informal relationships, effective transition was accomplished by codifying existing protocols, rather than by establishing completely new ones. An example of this was the allocation of diving services. Divers from various agencies have historically responded to the need for their services in an ad hoc, cooperative manner, with each event being organized at the time of need. Generally, the dive team with the specific capability that was most appropriate to the incident would act as the lead team, with the others operating under the lead team's direction. The new, formalized protocol has been established in much the same way, with the only substantive difference being that the request is initiated through a central office within the port area, and the appropriate teams are called in. According to the participants with knowledge of this arrangement, the formalized process works at least as well as the informal one it replicated.

While relationships between agencies were considered generally effective and functional, many participants saw them as being impeded by protection of organizational jurisdiction, and by competition for funding. Members recognized this kind of high-level rivalry within all the agencies involved in the study, even when working-level individuals enjoyed congenial and cooperative relationships among themselves. Although the sample size was small, the number of participants who identified incompatibilities between formal guidance and practical necessity for effective functioning was significant (see Table 2).

Table 2

Compatibility of Formal and Informal Procedures

Old Process:	Formal	Informal	No Process
Compatible	9	3	
Incompatible/ adequate		1	3
Incompatible/ adequate		4	1

Note. If a new process was seen to be similar to the one it replaced, it was characterized as compatible. If different, the question was whether the new one functioned adequately. If no previous process existed the same functionality question applied.

Existing formal processes of long standing were seen as compatible with functionality. Participants also believed that new, formal processes that largely adopted existing informal processes were acceptable. Likewise, some new processes that were seen as being incompatible with current practice, that is, they changed to new practices, were nevertheless acceptable. This was because, although different, they adequately served the purpose. Finally, though, there were new, formal processes that were seen as unacceptable, because they failed to serve the stated purpose in practical application.

Of the 21 new procedures noted by participants, there were four new ones that replaced existing, informal processes, but did not adequately accommodate the functionality of the processes they replaced. One new process was promulgated that had no predecessor, either formal or informal. It was identified as unacceptable, even though it was intended to address a newly recognized need. This was because the participant found that the new process did not function as intended.

These observations indicated that some problems existed in the development of new, formalized processes. Perhaps this is because of a lack of adequate investigation prior to introduction of new procedures. Alternatively, it may be caused by conflicts among agencies that resulted in compromises that sacrificed functionality for mutual acceptability. Either way, further study is warranted to make improvements in such policies and procedures.

One participant, E-5, noted that some agencies seem to cooperate better than others. The difference seen by this participant, as well as several others, as being a difference in agreement between high-level officials of the various agencies. In this individual's experience, there was one particular agency that did not cooperate well.

> We have jurisdiction over anything that goes down in the port, unless it belongs to the [local law enforcement agency with multiarea jurisdiction]. So, maybe we should be able to work past the [borders of the port] when we're onto something. But otherwise, we do just about everything.
>
> [On the protectionism issue, the same participant went on]:

> It doesn't happen very often, but they guard their turf. We don't have that problem with [neighboring port security], or with any of the other [agencies]. So, it's not a very big deal. It just looks bad. Maybe they think we want to push them out or take their money, or something. I don't know. (participant E-5, personal communication, November 5, 2014)

Based on the NVivo analysis, I was able to detect a high degree of consensus on the issue of jurisdictional protectionism (see Figure 2). Further, I was able to depict fragments of statements from the interview transcripts that contain references to the central theme. In this case, the references pertained to incidences of jurisdictional rivalries among high-level officials of the various agencies represented in the interviews.

The analyses depicted in Figures 2-5 consist of key concept words, surrounded by fragments of actual sentences of participants in their interviews. These fragments are intended to highlight the central concepts, rather than to explain them.

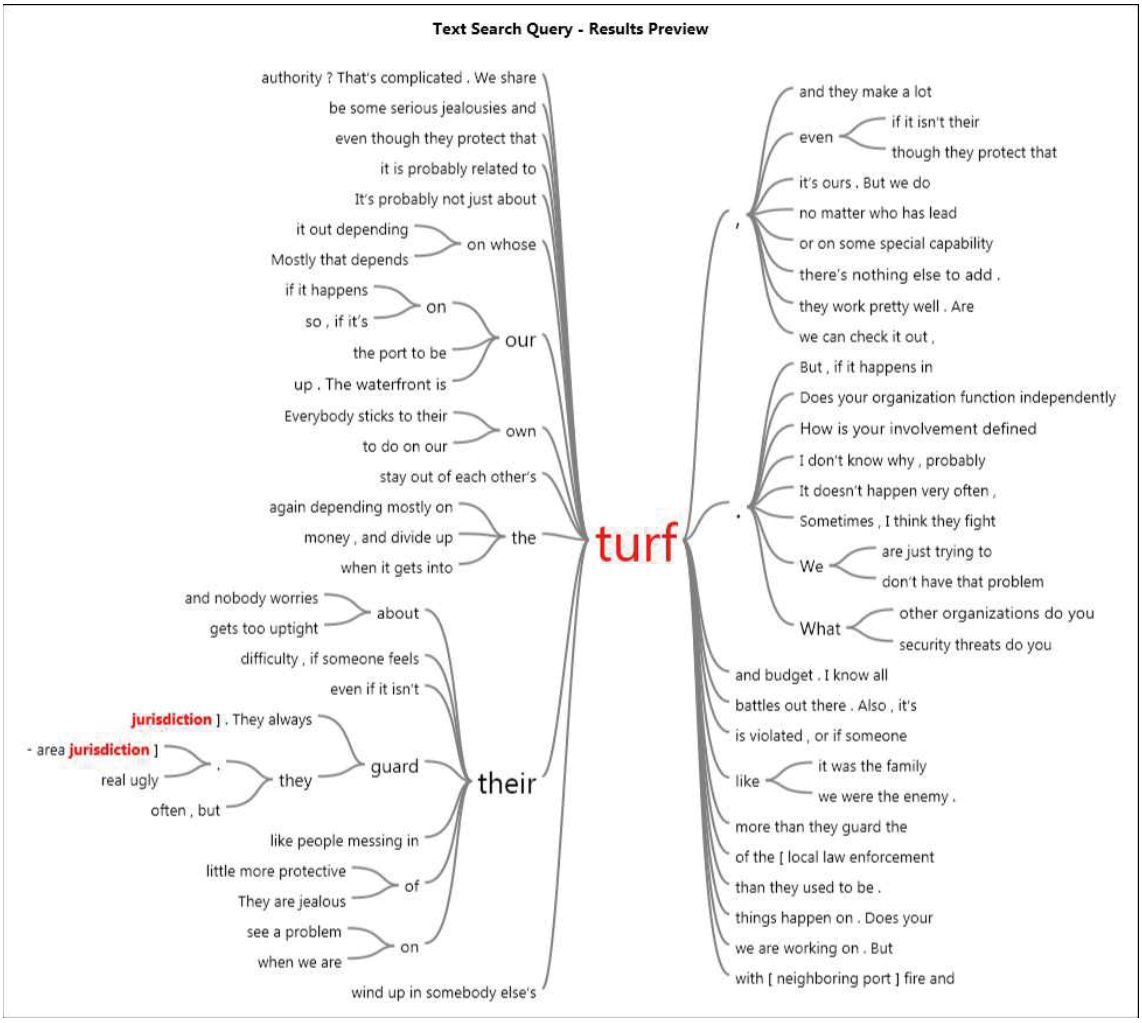

Figure 2. Jurisdictional protectionism, as expressed in participant interviews.

Participants viewed this kind of high-level rivalry as a result primarily of competition for funding, especially funding in the form of grants from DHS. As with the jurisdictional protectionism, a majority of participants expressed a belief that budget was a motivating factor in their parent organizations' attitudes toward interagency cooperation (see Figure 3).

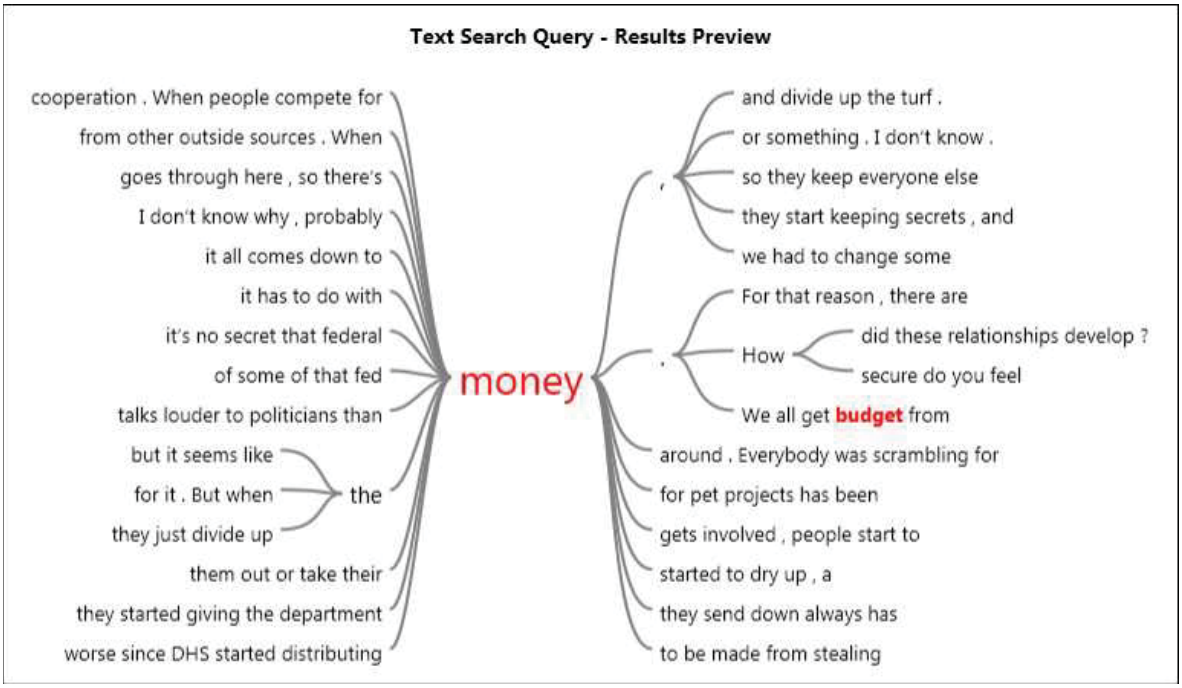

Figure 3. Participants' views about effects of competition for budget.

Theme 2: Informal Relationships. Participants acknowledged that informal relationships were a regular and necessary element of their working condition. Such relationships exist among peers within the same agency, and also between associates from different agencies. These relationships have formed as a means of accommodating situations that were not covered by official guidance. As participant R-3 expressed the informal relationships among peers within a single agency:

> There are a lot of routine jobs that just get done. It's a kind of tribal knowledge. Most of the work is covered by policies and procedures, but there are also some

> things that just require common sense. (participant R-3, personal communication, November 5, 2014)

The same participant described the situation with informal relationships between members of different agencies in a similar manner:

> There are a lot of activities here in the port that are routine. Even though we have policies and procedures that govern how we work, we also have some informal arrangements with several local agencies, especially port police and the fire department that we use for routine activities. (participant R-3, personal communication, November 5, 2014)

Many of the participants identified informal relationships, both within and outside of their home organizations. Motivational factors influencing these relationships tended to fit into three categories: existing personal relationships, habits that resulted from frequent operational contacts, and the necessity of pooling resources or relying on unique capabilities of some participants. These tended to be similar, whether the relationships existed within single organizations, across organizational lines, or in combination of internal and external relationships (see Table 3).

Table 3

Nature of Informal Relationships

Motivation:	Personal	Habitual	Necessity
Internal			
	6	3	4
External	11	16	12
Combination	1	4	2

Note. Specific numerical values resulted from somewhat arbitrary choices of relational words from the interview data set. However, use of synonyms would have produced similar numbers, with the same motivational factors.

RQ 2 and Related Themes

RQ2: How have informal working relationships formed, and what factors have kept them functioning?

Theme 3: Trust. The single most significant factor identified by participants that influenced informal, cooperative relationships, whether among members of a single organization, or across organizational lines, was the trust that existed between the individuals involved. The majority of participants specifically identified this factor, to such a degree that it emerged as a dominant theme I detected from NVivo (see Figure 4).

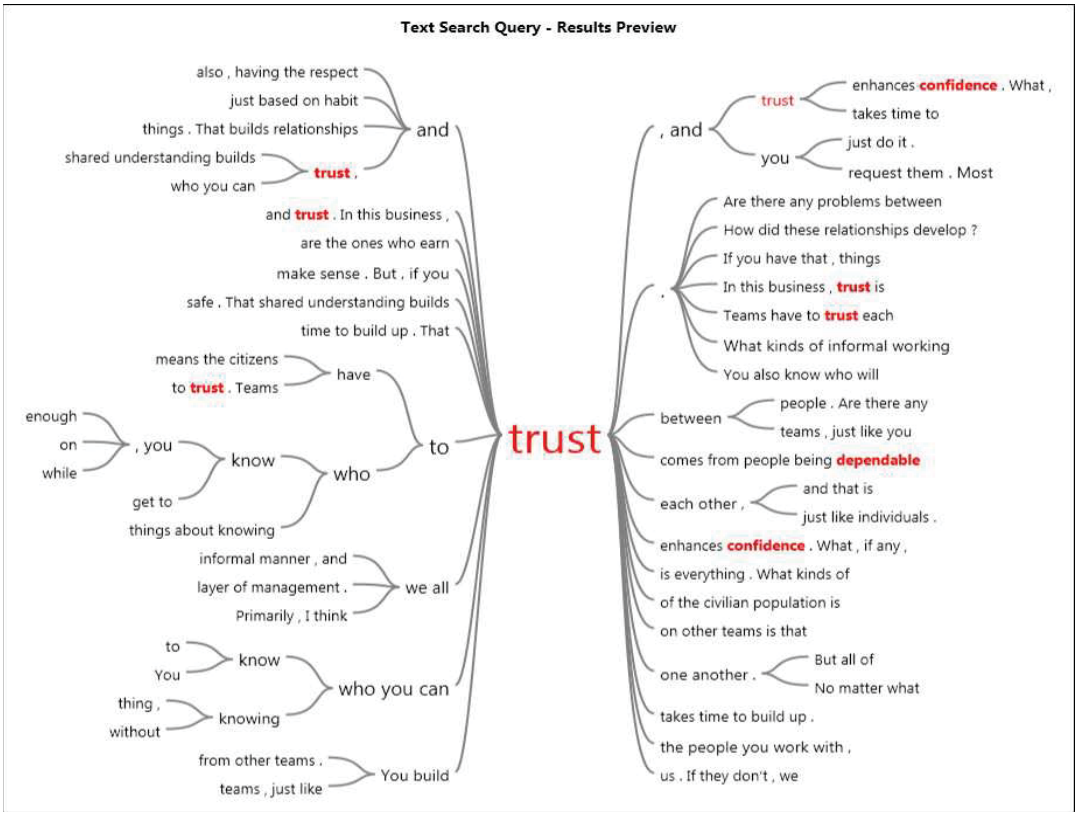

Figure 4. The role of trust in building cooperative relationships.

While trust often emerged as a byproduct of familiarity among participants within organizations, as well as across organizational lines, there were other influencing factors. Among these influencing factors were leadership and habitual integrity of individual members in the conduct of their interactions. Leadership, as defined by Schein (2010), was acknowledged and evident in many components of the study.

Whether formally defined, or exercised on individual initiative, leadership was evident and necessary for the successful operation of the organizations involved. Likewise, individual integrity of organizations' members was indispensable to the

development of mutual trust. Trust can also be a requirement of policy, in that some official procedures impose interdependency among participants. Although this kind of trust may be seen as directed, and thus insincere, it can lead to behaviors on the part of participants that result in earned trust.

Table 4

Sources of Trust

	Integrity	Leadership	Policy
Peers	20	4	2
Leaders	17	2	6
Subordinates	20		12

Note. There may be some overlap in the absolute numbers, because some trust begins with policy mandates, but develops into sincere trust, due to habitual integrity of the individuals involved.

As participant R-4 described these factors, both leadership and individual integrity were necessary to the functioning of an effective organization:

> Like any good team, all members cooperate and recognize the shared goals we all support. Under good leadership, cooperation and success are rewarded; so all members are motivated to generate efficiency and successful outcomes. Healthy

> working relationships naturally flow from those motivations. Many of us are acquainted with one another, through working on shared tasks, and through occasional social gatherings. Working relationships, both formal and informal, result from good people cooperating to achieve a common vision (participant R-4, personal communication, November 9, 2014).

Although this participant was in a formal leadership position, others expressed the same types of sentiments. As one working-level participant, identified as E-3, stated it:

> Somebody has to take the lead. If everybody else trusts [the leader], they do their part, and everybody's better off (participant E-3, personal communication, October 29, 2014).

Using NVivo, I was able to determine that leadership, while not as frequently cited as a critical factor, was sufficiently prevalent in the responses of the participants to generate its own relational tree (see Figure 5).

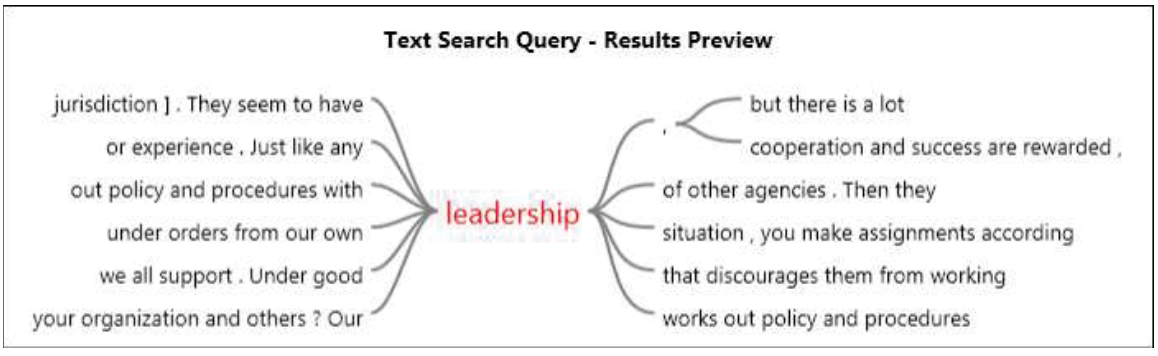

Figure 5. The role of leadership in building cooperative relationships.

Thus, leadership and individual integrity were shown to be interrelated, with each factor supporting and sustaining the other. This was exemplified in a statement by participant R-5, a leader who acknowledged the importance of leadership integrity in maintaining trust among organization members:

> We try to maintain an atmosphere of mutual respect, which includes regard for one another's professionalism. For that reason, we sometimes work in a relaxed and informal manner, and we all trust one another. But all of our working relationships must still conform to the standards that are promulgated for us (participant R-5, personal communication, November 9, 2014).

Good leaders were seen to inspire confidence in those who were led. This confidence spread across organizations. As participant S-2 stated:

> Every force has good people on it. We all look out for each other. (S-2)

Inspired individuals tended to act with integrity, which enabled leaders to continue to function in their leadership roles, whether formal or informal. As a result, mutual trust and cooperative relationships continued.

RQ 3 and Related Themes

RQ3: What kinds of security threats were recognized within the research environment, and how were they identified and assigned for action?

Theme 4: Security Threats. Participants identified eleven categories of security threats. One or more participants acknowledged most threats as part of their assignments,

and viewed those to be appropriate to their agencies and individual jobs. A general sense of satisfaction with assignment and resources for the assignment was prevalent.

The single exception was cyber crime. Of the five participants who acknowledged awareness of it as a threat, only two identified cyber threats without having to be prompted by the interviewer. The other three responded to a researcher follow-up question regarding cyber crime. None of the participants believed they personally had a role in combating cyber crime (see Table 5).

Table 5

Types of Security Threats Identified by Participants

Type of Security Threat	Frequency	Assigned, Y/N
Terrorism	16	Y
Smuggling	15	Y
Drugs	14	Y
Burglary	8	Y
Street Crime	7	Y
Arson	6	Y
[Cyber Crime]	[2]	[N]

Note. Chart reflects only threats identified by five or more participants. Several other types of threats were identified, and all were assigned to one or more participants for action. Cyber crime is listed here, because it was the only threat not assigned to any participant.

Most of the security threats, such as smuggling, burglary, arson, and sabotage were identified by, and assigned to, personnel and agencies generally concerned with a specific type of threat. Several threats, such as terrorism and smuggling, were assigned to more than one organization. Other threats, such as burglary or traffic violations, were

assigned specifically to only one agency for each jurisdictional area. This is not to say that any agency was specifically prohibited from helping to mitigate these activities within their areas of jurisdiction, but primary responsibility was clearly assigned.

Theme 5: Additional Threats. When asked about additional threats for which participants believed they should be responsible, most replied that no additional threats would be appropriate for their type of job. Of those who did believe some added responsibilities would be appropriate, the most common answer was not addition of new threats, but authorization to act outside the boundaries of their normal operating area. Although this was not generally stated as a desire for additional assignments, or for broader functional operations, it was emphatically declared. It was stated rather as a practical matter that would enhance operational effectiveness of existing procedures. As one law enforcement officer, E-4, stated:

> We already have responsibility for any kind of threat response, but we should have less restriction on how to respond, especially when it comes to our geographical jurisdiction. I don't mean just the right of hot pursuit. I mean that if we see something that is outside our boundaries, we should be free to exercise professional discretion to investigate it. As it is, there are things that we can only report, but can't actively pursue. I have personally seen situations where a suspect got away, because he knew he had been spotted (participant E-4, personal communication, October 29, 2014).

Table 6

Additional Desired Threat Jurisdiction

Threat Jurisdiction	Geographic	Qualitative
Enforcement	6	1
Regulatory		2
Safety	2	2

Note. The desire for wider geographic jurisdiction referred to the ability to investigate or pursue issues beyond current limits. Participants who expressed a desire for additional qualitative jurisdiction identified the same issues: arrivals from domestic sources and cyber crime.

Theme 6: Unaccounted Threats. Although most participants believed their assignments to be generally appropriate to their agency and job, there was some controversy about the priorities and concentration of resources associated with mitigating the various threats. For example, three participants, representing two different agencies, believed that there was not enough emphasis on materials coming into the port from the landside, loaded on trucks or rail cars, or empty cargo containers to be returned to their country of origin. The participants felt that there was an opportunity for sabotage or other

threats to result from insufficient screening of materials delivered from within U.S. territory.

This is not to say that there were no provisions for detecting inappropriate material entering from the landside. Official policies and procedures were in place to address this kind of issue. Observations did reveal that the policies and procedures seemed to be a routine element of normal port operations. Even so, participants such as C-1, a civilian security manager for a large material staging, warehousing, and shipping facility, did express concern that these policies and procedures were not sufficiently detailed and thorough to adequately protect from this kind of threat.

> Theft and hijacking are big worries in our facility. There is a huge amount of valuable cargo that goes through here, so there's money to be made from stealing it. That is our biggest worry (participant C-1, personal communication, November 5, 2014).

Table 7

Unaccounted Threats

	Regulatory	Enforcement	Safety
Trucks	1	4	3
Rail	2	1	
Autos		6	
Other		2	

Note. Most of the concern for unaccounted threats was related to lack of adequate tracking, regulation, or inspection of incoming materials from the domestic landside. The *other* category referred to pedestrian, bicycle, and other nonmotorized traffic.

There were also unexpected gaps in responses concerning the potential for cyber terrorism. In addition to this, there was clearly a lack of recognition of the significance of the Fusion Center. All of these issues are covered further in Chapter 5, under Recommendations.

Summary

As intended, I identified a combination of both formal and informal working relationships that operate within the research environment. I found the formal relationships to be governed by appropriate, documented command media, and that

personnel recognized and generally followed them. Where formally mandated relationships were not sufficient, or were inappropriate to conditions encountered in the working environment, participants developed relationships among themselves to accommodate the situation.

These relationships formed through perceived necessity among functional personnel in the normal course of their work. Familiarity and trust grew among the participants, which provided them with the confidence to act, as they deemed necessary, even though some of their actions were not formally sanctioned by documented policies and procedures. The key element influencing development of these working relationships was the element of mutual confidence and trust.

The initiative of individuals exercising leadership qualities, while helpful in mitigating some negative factors, was seen as not always being sufficient to overcoming all structural, situational, or organizational barriers. Difficulties in maintaining efficient, cooperative relationships were seen by the participants as being the result of competition among organizations for jurisdictional authority and access to outside sources of funding.

Generally, there was consensus among participants about the types and variety of security threats they faced in protecting the port. Responsibility for mitigating these threats was appropriate to the missions of the home organizations and individual job descriptions. Some gaps in emphasis were recognized by participants, who believed that additional resources should have been focused on inadequately treated potential threats.

Other threats, such as vulnerability to cyber attacks, were not generally recognized as major responsibilities.

The implications of these gaps, and suggested actions to fill them have been presented in Chapter 5. The final chapter of this work also contains conclusions from the current study. Additionally, it includes acknowledgement of limitations and unresolved issues from the current study, and recommendations for further actions and research.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this qualitative case study was to explore issues that can hamper efficiency of security agency operation and collaboration, and to identify actions that have enhanced collaboration. A search of professional literature has revealed that exploration of this subject is both desirable and useful, and that there has not been sufficient study of the factors that influence cooperative relationships among the many official agencies responsible for security in the nation's transportation hubs.

Specifically, the large seaport that has been the subject of this study, has not been studied from this perspective, even though multiple agencies must interact and work in symbiosis, to ensure the safety of the port, while respecting the rights of the various people and organizations who function within it. I have found that many inter organizational relationships exist—some that were mandated by official authority, and some that have developed through voluntary association among individuals and groups– but that there exist issues that limit the effectiveness of the relationships. Some of these issues relate to a lack of cohesive guidance from official authority, some from conditions in which official guidance mandates interactional modes that hamper effective functioning of working level security personnel, and some that expend resources inefficiently, while failing to fulfill the intended purpose. Finally, while most organizations and individuals involved displayed a conscientious intention to perform their duties in a manner that achieved security without unnecessarily intruding upon the rights and freedoms of the people who use the port facilities, occasional incidents have

arisen in which such intrusions have occurred, and the potential for more, and increasingly serious intrusions have continued to exist.

There was evidence of a general recognition among the organizations of the necessity of maintaining the trust of the protected public. Several interviewees acknowledged that their effectiveness depended on trust and cooperation from the population. Some of the observations also revealed courteous, and in one case, active cooperation between an agency member and a private citizen. Should this trust and mutual respect deteriorate, agency members acknowledged that the results would be very negative the protectors and protected, alike.

Interpretation of the Findings

The kinds of cultural norms and models described by Schein (2010) proved to be extant in the current study environment, having been fostered and perpetuated in the manner that Schein predicted. Furthermore, as Schein described the conditions that must exist in order to infer the presence of organizational culture, the observations must reveal that the norms of the group are recognized by the members as appropriate for accomplishment of shared goals and intentions. The norms must also be seen as sufficiently valuable to be included as part of the orientation of new members who join the group. The presence of such norms was evidenced in various ways throughout the study, perhaps best exemplified by the response of participant S-5 to a question about these norms:

> We all have our own ways of working together. I mean, you can't work with the same crew all the time and not have regular habits. Usually, that is in some of the routine jobs, especially records and reports. Some [personnel] are better at some of the jobs, but not as good at others, so we divide things up. As long as everybody gets fair treatment, it works. It just comes from working together a long time. Newbies [sic] come in, and they have to get used to it, and we have to get used to them. Of course, they usually start with some of the jobs nobody wants, but we try to keep it fair. If it gets too out of line, people stop getting along, and that's bad for everybody (participant S-5, personal communication, November 2, 2014).

Through the literature search, I discovered reports that added some examples of research applications of Schein's models. For example, Solansky and Beck (2009) found that some interorganizational cultures developed shared acknowledgement of the importance of collaboration among organizations. These organizations tended to achieve increased effectiveness and shortened response times in addressing threats. This shared acknowledgement, or belief, was seen to manifest itself in collective commitment to collaboration. This cooperation extended, when necessary, to the protected public, as well.

The professed commitment, identified in Solansky and Beck's paper, was consistent with the second level of culture, as described in Schein's book. This phenomenon was corroborated in Blair and Janousek (2013), who found that cooperative

interagency relationships tend to be informal. Even when starting as formal, directed relationships, Blair and Janousek (2013) discovered that these relationships tended to evolve, over time, into informal interactive protocols that participants found to be functional.

A negative, but useful example of research that can be related to Schein (2010) was Garrett's (2010) study, which found that failures of large, interagency organizations to develop shared acknowledgement of the need for collaboration, resulted in substantial inertia and general dysfunction in the larger organization. Garrett's descriptions of these problems were comparable to the understood, tacit sorts of belief (or lack thereof) existing in the third cultural level described in Schein's book. Specific observations cited in the Garrett study indicated that this underlying assumption was lacking. Absence of this shared assumption was consistent with the behavioral actions contained in the first level of culture described by Schein. Schemeil (2013), found that organizations tended to find new modes of cooperation as a means of surviving changes in their organizational mandates.

Garrett (2010) viewed the observed behaviors to be both symptoms and results of the failure of organizational leadership to foster the kinds of cultural development necessary for effective functioning of interagency organizations. The leadership failures were examples of the type described theoretically in Schein's (2010) book. Finally, Chenoweth and Clarke (2010) found that existing organizational cultural norms, which were described in a manner that was consistent with Schein's model, increased the

likelihood that multilevel, and multiagency organizations would coalesce successfully, to make efficient use of available resources. In general, the literature search revealed that the organizational culture models provided by Schein (2010) would serve effectively as a conceptual framework for the entire research project.

A final contribution from Schein's (2010) work has been the role of leadership in making organizational intentions work in a practical manner. Whether in the formal, hierarchical structure of the organizations, or within ad hoc work groupings, or with informal relationships that have formed, leadership was consistently acknowledged during the interview process. This effect was occasionally evident during the observation phase of the study. Even though opportunities for directly identifying leadership actions were rare, there was evidence of leadership influences on organizational behavior, in the manner that Schein described.

Discussion with participants on the subject of the types of security threats they recognized revealed that they were generally aware of, and felt responsibility for mitigating, the threats Lutz, Roell, and Thiele (2013) defined. These threat types included terrorism, smuggling, and crimes against persons or property. This shared recognition and commitment tended to enhance cohesiveness among members of the organizations included in the study, and helped maintain a shared sense of purpose. A clear deficit in threat recognition was the general lack of focus on the potential for cyber threats. Even though all participants exhibited a significant dependence on electronic, networked devices for their routine functioning, few of them mentioned cyber security as a threat,

and none expressed any personal responsibility for it. As Kramek (2013) discovered, many people in security jobs lack this recognition, although nearly all have an opportunity to at least monitor the performance of their own equipment for evidence of cyber intrusion or disruption. I noted a similar lack of awareness among participants in the current study.

One interesting phenomenon noted in the study related to the work by Chalk and Rosenau (2004), who found that security agencies, especially those in the United States, often have difficulty coordinating and cooperating, because of a variety of factors. These factors include variations in priorities and policies, limited jurisdictions, and political competition among the agencies involved. While these same kinds of factors were evident in the research environment, there was evidence of a considerable amount of mitigating activity. Some of this took the form of official policy coordination among local authorities, but much of it was achieved through personal initiative of individuals and small groups, who recognized the mutual benefit of agreeing to, and maintaining such informal protocols.

Chappell and Gibson (2009) noted a similar issue, and found that considerable controversy exists concerning the compatibility of large-scale security maintenance with the practice of community policing. In the present study, a philosophy of community policing was evident among many of the participants, and was also recognized in official doctrine. In this case, the evidence supported an argument in favor of community policing, in that the process has been generally successful, both in minimizing locally

based crime, and in maintaining effective focus on the larger scale issues of terrorism and smuggling. Because no evidence emerged to indicate that there were any conflicts attributable to community policing practices, the data have supported the argument in favor of continuing the policy in the port.

As Parks et al. (2013) discovered, coordination among agencies, and communication with affected members of the agencies, is vital when making policy or major procedural changes. Without this coordination and communication, policies are likely to be inconsistently perceived by organization members, with a resulting negative effect on perceptions of the public who are affected by their implementation. Overman et al. (2014) found that negative perceptions by the protected public can result in mistrust and loss of the kind of willing public cooperation on which effective security measures depend. According to the Overman work, thoughtful and thorough coordination of proposed policy changes are vital to their successful implementation, which, in turn, result in public benefit from the changes.

Some significant negative issues also emerged in the course of the study. One was the kind of problem explored by Woods and Bowman (2011), in which competition among agencies for federal funding and other types of sponsorship can be a major impediment to cooperation among agencies. This was definitely evident in the views of most of my study participants, many of whom cited either competition for money or jurisdictional authority as factors that interfered with their ability to openly cooperate with peers from other agencies. While some agencies had found ways to cooperate

effectively, others did not. Resource and jurisdictional competition was clearly the dominant factor in the noncooperative situations.

Other negative findings included the lack of emphasis on cyber security, mentioned previously, and the limited use, among study participants, of the resources devoted to the Fusion Center. As Leithauser (2012) found to be widespread among such facilities, there was little evidence in the study environment of any significant use of this entity among security personnel at the working level.

The *prima facie* evidence is very strong that the security operations in the subject port are effective and appropriate to the prevailing conditions. This is because no major incidents have occurred, despite the fact that there is credible evidence that the recognized threats remain. On the other hand, most of the agencies involved in the study have had the unfortunate experience of having some of their members lose their lives in the line of duty. Clearly, the threats remain, and vigilance against them must be maintained.

For these reasons, any actions that may enhance the ability of the people who are charged with the responsibility of safeguarding the port facilities to carry out their duties without undue risk to themselves are clearly welcome. At the same time, the safeguarding must be done in a way that recognizes the rights of people engaged in legitimate activities to go about their business with minimum impediment. These vital, simultaneous, and sometimes conflicting tasks must continue. If not, the public trust on which effective security depends would erode, with seriously negative consequences.

Limitations of the Study

This study has been limited by a number of factors including sample size, time, and geography. While necessary for practicability of the study, they did result in some limitations to the breadth and detail of the conclusions. Each of these limitations will be treated separately.

First among limitations was the limited number of participants interviewed. Although an adequate number have been included for the purpose of engaging a representative sample, it has been, nevertheless, a sample, which is subject to the limitations of sampling techniques. While the consistency of resultant data has revealed that the sample has been adequate, it is still possible that a larger sample might render some differences in findings.

Time has also been a limiting factor. As stated in the discussion of research design, the timeframe allocated for data collection has been limited to approximately two months. This has resulted in various limits, especially in the case of observation. Many of the kinds of incidents to which participants and their parent organizations must respond occur only rarely. In fact, only three of the observed incidents required more than one organization to respond, and only seven incidents of nonresponse activities, such as lunchtime interactions or other collective activities, were observed during the course of the study. All of the observed activities were consistent with the outcomes of interviews, and were consistent with the general findings of the study. Even so, additional

observations, conducted over a longer period of time might have generated data that would have had an effect on findings and conclusions.

The decision to limit the study within the boundaries of a single port also imposed limits on data collection. The waterways used by the subject port are also used by the neighboring port. Although no evidence of conflicting data attributable to the other port emerged during the course of the study, such conflicts may have existed and remained undetected. There may also have been interactions at the other port occurring among members of organizations from both ports. Observations of such interactions may, or may not have had a meaningful effect on interpretation of the total data set.

A study encompassing a larger geographic area, involving a greater number of organizations, over a longer period of time, might possibly yield some differences in results. While the evidence gathered during the current study was sufficiently consistent and compelling to indicate that it is probably valid, a larger scaled study would be likely to provide amplifying information, with additional conclusions and indications that would enhance the value of the pursuit.

Recommendations

Further research into some of the issues treated in this study could yield additional benefit. Although interview responses were generally consistent with one another, a larger sample size might yield additional useful detail. Because of the time limitation, additional observations might provide insights into specific kinds of interactions resulting from actual incidents that would require large scale, cooperative action by multiple

agencies. Finally, further study beyond the geographical boundaries of the selected research environment would probably provide interesting results. This could be especially true if a similar study were to be done in the neighboring port, using similar approaches and techniques.

I also found unforeseen issues that were beyond the scope of the current work, and exploration of these issues warrants further study. One such issue is the matter of cyber security. Specifically, a detailed look at the kinds of activities to mitigate the cyber threats would certainly be valuable. As Solansky and Beck (2009) recommended, examination of efforts to coordinate activities among agencies might be especially valuable. Similarly, further study of the actual role of the Fusion Center, and the manner in which its capabilities and resources are used would probably prove useful. The suggestions offered by Caldwell (2012), concerning procedural integration of Fusion Center capabilities with other security activities, were found to be applicable here, and, as Caldwell had noted in other environments, should receive further attention.

Finally, as Adams and Balfour (2010) noted, it is very important to be aware of the risks of institutional competition for resources and its potential effect on cooperative action. Several participants acknowledged the presence of this kind of competition. The implications of such competition could be profoundly negative, and will be discussed below.

Implications

All of the participants in the study expressed a sincere recognition that the principal goal of their jobs and their organizations was to maintain the safety of the public, in their persons, their property, and their legitimate activities. Measures taken to accomplish the necessary level of security are, in themselves, forces of social change. The question of whether the resulting social change will be positive or negative hinges largely on the manner in which these security measures are implemented, public perception of the appropriateness of the measures, and, of course, the effectiveness of the measures.

To ensure that these measures are imposed and received in a positive way, it is necessary that management of the processes for providing security be established and maintained wisely. These issues were clearly demonstrated during the research by Parks et al. (2013), who discovered that organizational leaders could exert a strong influence on the perceptions of public employees, depending on the manner in which they presented and enforced active and interactive protocols. Without such positive influences, a frightening, but very possible scenario could be that some major incident would generate political pressure to make sudden, substantial changes in the way security is maintained. If high-level institutional pressures were to cause hasty and potentially inappropriate decisions, the consequences could be tragically negative. The importance of this issue was evident at the research site, where agency members acknowledged their dependence on a cooperative public.

Such claims were evident in the findings of Overman et al. (2014), who likewise found that high-level negotiations for changes in policy or interactive protocols should be thoroughly worked out in advance of presenting them to lower level organizations and personnel, to help prevent friction and resistance to change incorporation. Should security practitioners at the working level find themselves in a position of having to implement new policies they do not believe to be effective, or which increase the personal risks to which they are exposed, the level of commitment to public safety which they have shown to be paramount in their minds would inevitably diminish. Without these preparatory measures and sympathetic direction from leadership, frustration and fear would begin to replace enthusiasm.

Such frustration and fear would inevitably affect the manner in which security practitioners would interact with the very public they were charged with protecting. Public perceptions of their protectors would be negatively affected, and the level of trust and cooperation that presently exists would diminish. As stated in the Findings section, cooperation and tolerance of security measures by the general public are indispensable to effective security activity. In such a scenario, the social change imposed by the recognition of growing security threats would be decidedly negative (see p. 113).

Instead, it is hoped that findings from studies such as this one will enhance the ability of policy makers to recognize factors that have produced favorable results, as well as factors that have not. For example, recognizing interactive protocols that are already in place and functioning satisfactorily could help smooth the introduction of additional tasks

or security measures. I have found this kind of recognition to have positive results in the present study. On the other hand, unrealistic expectations of the value of new measures can result in resignation and cynicism among personnel who are expected to use them. This has also been observed in the present study.

With this kind of information at their disposal, policy makers should be better prepared to respond appropriately to any change in the security environment for which they are responsible. In such a case, the vital trust by the protected public in the necessary laws and regulations, as well as in the people who must enforce them, will remain secure. With this trust and cooperation maintained, the ability of the protectors and the protected to carry on their legitimate activities will be minimally affected by unavoidable outside forces. This would be the optimum scenario in a society that recognizes the necessity to remain safe, while still preserving, to the greatest extent practicable, their individual and collective freedoms.

Conclusion

My conduct of this study has proved to be both enlightening and gratifying. It has been enlightening in that it has revealed that a complex mix of organizations, with collective responsibility for managing an even more complex set of tasks can work effectively and efficiently. This has proved to be largely attributable to the many people who each take their personal responsibilities seriously, and who display a high degree of professional integrity in carrying out their duties.

The experience has been gratifying, because, even though ongoing efforts have been effective in preventing major incidents of crime and terrorism, my work has revealed that there are some kinds of activities and processes that could be improved. The improvements, if implemented, could materially enhance the ability of the organizations and individuals to perform their work even better than they already do. Additionally, these kinds of improvements would also aid the addition of new responses to new threats as they emerge. As a result, the society that enjoys the protection they are currently receiving could continue to reap the quiet and mostly invisible benefit of a secure and largely unobtrusive protective environment. Any social change necessitated by current and future security threats would thus continue to be substantially positive.

Clearly, security of the port continues to be effectively maintained. This is due to the work of competent and dedicated people, who are committed to the jobs they are assigned to do. Even so, there remain threats that should be addressed more actively. Fortunately, there are people and processes in place that, given adequate support and direction, should prove equal to the task.

References

Adams, G., & Balfour, D. (2010). Market based government and the decline of organizational ethics. *Administration and Society*, *42*, 615–647. doi:10.1177/0095399710381347

Alitok, T. (2011). Port security/safety, risk analysis and modeling. *Rutgers University Ann Oper Res*, *187*, 1–3. doi:10.1007/s10479-011-0849-8

Blair, R., & Janousek, C. (2013). Collaborative mechanisms in interlocal cooperation: A longitudinal examination. *State and Local Government Review, 45*(4), 268–282, doi:10.1177/0160323X13511647

Belzer, M., & Swan, P. (2012). Supply chain security: Agency theory and port drayage drivers. *Economic and Labour Relations Review*, *22*(1), 41–44. doi:10.1177/0160323X13511647

Caldwell, S. (2012). Coast Guard needs to improve use and management of interagency operations centers. *United States Government Accountability Office Report to Congressional Requesters.* Retrieved from http://www.gao.gov/GAO-12-202

Chalk, P., & Rosenau, W. (2004). *Confronting the enemy within.* Santa Monica, CA: RAND Corporation.

Chappell, A., & Gibson, S. (2009). Community policing and homeland security policing: Friend or foe? *Criminal Justice Policy Review*, *20*, 326–343. doi:10.1177/0887403409333038

Chenoweth, E., & Clarke, S. (2010). All terrorism is local: Resources, nested institutions, and governance for urban homeland security in the American federal system. *Political Research Quarterly*, *63*, 495–509. doi:10.1177/1065912909334426

Creswell, J. (2007). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Diefenbach, T. (2009). Are case studies more than sophisticated storytelling? Methodological problems of qualitative empirical research mainly based on semi-structured interviews. *Qual Quant*, *43*, 875–894. doi:10.1007/s11135-008-9164-0

Dulles, A. (2006). *The craft of intelligence.* Guilford, CT: Lyons Press.

Eriksson, J., & Rhinhard, M. (2009). The internal-external security nexus. *Cooperation and Conflict: Journal of the Nordic Security Studies Association*, *44*, 243–267. doi:10.1177/0010836709106215

Eski, Y. (2011). ”Port of call”: Towards a criminology of port security. *Criminology and Criminal Justice*, *11*, 415–433. doi:10.1177/1748895811414593

Feldt, L., Roell, P., & Thiele, R. (2013). Maritime security-perspectives for a comprehensive approach. *Institute for Strategic, Political, Security and Economic Consultancy, 222,* 1–25. Retrieved from http://www.ispsw.de/fdis/222

Garcia, A. (2011). Cognitive interviews to test and refine questionnaires. *Public Health Nursing*, *28*, 444–450. doi:10.1111/j.1525-1446.2010.00938.x

Garrett, T. (2010). Interorganizational collaboration and the transition to the department of homeland security: A knowledge analytic interpretation. *Administration & Society*, *42*, 343–360. doi:10.1177/0095399710362718

Giblin, M., Schafer, J., & Burruss, G. (2009). Homeland security in the heartland: Risk, preparedness, and organizational capacity. *Criminal Justice Policy Review*, *20*, 274–301. doi:10.1177/0887403408323762

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12–17. doi:10.7748/nr2013.03.20.4.12.e326

Johnson, W. (2009). *Thwarting enemies at home and abroad.* Washington, DC: Georgetown University Press.

Kempfer, H. (2011). Maintaining security of American infrastructure. *Infrastructure Liaison Officer.* Lecture conducted from US Department of Homeland Security, San Clemente, CA.

Leithauser, T. (2012). Senate report on DHS fusion centers provokes debate about data sharing. *Cyber Security Policy Report,* 1. Retrieved from http://search.proquest.com/docview/1124554693?accountid=14872

Lisle, D. (2013). Frontline leisure: Securitizing tourism in the war on terror. *Security Dialog*, *44*, 127-146. doi:10.1177/0967010613479426

Martella, R., Nelson, R., & Marchand, N. (1999). *Research methods.* Needham Heights, MA: Allyn and Bacon.

Monahan, T., & Palmer, N. (2009). The emerging politics of DHS fusion centers. *Security Dialog*, *40*, 617-636. doi:10.1177/0967010609350314

Nau, H. (1995). *Trade and security.* Washington, DC: American Enterprise Institute.

Oliver, W. (2009). Policing for homeland security: Policy & research. *Criminal Justice Policy Review*, *20*, 253-262. doi:10.1177/0887403409337368

Olson, J. (2006). *Fair play.* Dulles, VA: Potomac Books.

Oskarsson, S., Svensson, T., & Oberg, P. (2009). Power, trust and institutional constraints: Individual level evidence. *Rationality and Society*, *21*, 171-195. doi:10.1177/1043463109103898

Overman, S., van Thiel, S., & Lafarge, F. (2014). Resisting governmental control: How semi autonomous agencies use strategic resources to challenge state coordination. *International Review of Administrative Sciences, 80*(1) 172-192. doi:10.1177/0020852313509534

Parks, C., Joireman, J., & Van Lange, P. (201). Cooperation, trust and antagonism: How public goods are promoted. *Psychological Science in the Public Interest, 14*(3) 119-165. doi:10.1177/1529100612474436

Pfeffer, J. (1998). *The human equation.* Boston, MA: Harvard Business School Press.

Roberts, A., Roberts, J., & Liedka, R. (2012). Elements of terrorism preparedness in local police agencies, 2003-2007: Impact of vulnerability, organizational characteristics, and contagion in the post-9/11 era. *Crime and Delinquency*, *58*, 720-747. doi:10.1177/0011128712452960

Sandoz, J. (2012). Maritime security sector reform. *United States Institute of Peace – Special Report.* Retrieved from http://www.usip.org/files/resources/SR306.pdf

Schein, E. (2010). *Organizational culture and leadership.* San Francisco, CA: Jossey-Bass.

Schemeil, Y. (2013). Bringing international organization in: Global institutions as adaptive hybrids. *Organization Studies.* doi:10.1177/0170840612473551

Sims, J., & Gerber, B. (2005). *Transforming US intelligence.* Washington, DC: Georgetown University Press.

Singleton, R., & Straits, B. (2010). *Approaches to social research* (5th ed.). New York, NY: Oxford University Press.

Solansky, S., & Beck, T. (2009). Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. *Administration and Society*, *40*, 852-875. doi:10.1177/0095399708326345

Stake, R. (1995). *The art of case study research.* Thousand Oaks, CA: Sage.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Thousand Oaks, CA: Sage.

Trochim, W. (2001). *The research methods data base.* Mason, OH: Thompson.

Woods, N., & Bowman, A. (2011). Blurring borders: The effect of federal activism on interstate cooperation. *American Politics Research*, *39*, 859-884. doi:10.1177/1532673X10397923

Yin, R. (2009). *Case study research design and methods.* Thousand Oaks, CA: Sage.

Appendix A: Consent Form

This consent form will be used for all participants. Anyone who signs a form will receive a copy of the form with both the participant and interviewer's signatures.

Consent Form

You are invited to take part in a research study of inter-agency security operations within the area of the seaport. To conduct the study, it is necessary to interview and observe people whose professional duties include activities necessary for maintaining security in the port and its environs. Because of your position in a security organization, you have been identified as someone who would be appropriate to participate in the study, if you are willing to do so. This form is part of a process known as "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by Ed Levy, who is a doctoral student at Walden University.

Background Information:

The purpose of this study is to describe the manner in which the many agencies involved in providing port security interact. This includes formal relationships which are defined by official policy, and informal relationships that form among professional colleagues who cooperate with one another in the normal course of their work.

Procedures:

If you agree to be in this study, you will be asked to:

- Be interviewed about the nature of your duties and the kinds of organizational interfaces you have with people from other organizations. The interview is brief, and should not require more than thirty minutes of your time. In some cases, a follow-up interview may be needed, so you can help explain or clarify some information that the researcher obtains during the course of the study.
- Be observed in your work environment, perform your normal duties.
- Suggest inclusion of official, publicly-releasable documentation that provides guidance for you in executing your duties and interfacing with other organizations.

Here are some sample questions:

- What is your job title?
- To what security organization do you belong?
- What other organizations are normally involved in your work?
- How well do you think the cooperative relationships work?
- If there are issues, what do you think causes them?
- How do issues usually get resolved?

Voluntary Nature of the Study:

The study is voluntary. Everyone will respect your decision, whether you choose to participate or not. No one at any of the agencies involved will treat you any differently if you decide not to participate. If you decide to join the study and change your mind later, you can still change your mind later. You can leave the study at any time.

Risks and Benefits of the Study:

Because this is a non-intrusive study, and neither you nor anyone else will be asked to do anything other than your normal work activities, the only risks that might be incurred are potential risks to privacy. These risks may be divided into two categories:

Risks to your personal privacy.

Risks of disclosure of information that your organization may consider sensitive.

Protective measures to safeguard your personal privacy are described in the Privacy section below.

Protection for organizational information will be provided by special measures to keep observational and interview data secure, and by including key individuals within the

affected organizations in the process of vetting the observations and findings, in order to prevent inadvertent disclosure of sensitive information.

Privacy:
Any information you provide will be kept anonymous, and will not be attributed to you in any report or document. Your identity will be assigned a code which will not have any link to other documents associated with the study report. Further, all participants, even those who are willing to be identified, will be kept anonymous. This is to prevent inadvertent "identification by omission" or other deductive means of identifying participants. Data will be kept for at least five years, and all protections, both documentary and systemic, will be maintained throughout that time.

Contacts and Questions:
You may ask any questions you have now. If you want to talk privately about your rights as a participant, you may call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is X-XXX-XXX-XXXX, extension XXXXXX. The researcher will give you a copy of this form to keep, and you should keep it for your records.

Printed name of participant: _____
Date of consent: _____
Participant's signature: _____
Researcher's signature: _____

Appendix B: Interview Worksheets

The following worksheets to be used in the interview process.

INTERVIEW WORKSHEET

- What is the role of your organization in the port?
- How does your organization share security responsibility with other organizations?
- What other organizations do you interface with?
- How are decisions regarding security operations made between your organization and others?
- Does your organization function independently in security work, or does your organization take direction from some other authority?
- Are you aware of any high-level policy that comes from outside your organization? If so, where does it come from?
- What kinds of informal working relationships have you formed with members of your own organization?
- How did these relationships develop?
- What kinds of informal working relationships do you have with members of other organizations?
- How did these relationships develop?
- Are there any problems between the informal working relationships and the official direction that governs your work?
- What security threats do you know about that could affect the port?

- Among these, which ones are you involved in mitigating?
- How is your involvement defined and assigned to you?
- How secure do you feel in your working environment?
- What factors contribute to your personal feelings about security?
- What, if any, security threats do you think should be added to your assigned duties?
- If there are additional threats, why should you be involved with them, and what would be your role in mitigating them?

Appendix C. Sample Introduction Letter for Potential Participants

Dear _____

As part of my academic program at Walden University, I am conducting a study at the Port, concerning interagency coordination for maintenance of security within the Port environment. Because of your position in the research environment, you may be able to help me, by answering some questions about the mission and tasks of your organization.

Should you choose to participate, I will contact you to arrange a meeting, during which I will explain details of my study, and ask you some questions that will help me gain understanding of the security situation at the Port, and the manner in which security is maintained. Your participation is, of course, totally voluntary, and your identity and participation will be kept completely confidential. At the time of our meeting, I will provide you with a privacy guarantee document, and that we will each sign and retain a copy.

Your participation will not only be helpful to me in the conduct of my study, but may also help identify factors that enhance Port security, and perhaps also factors that detract from it. But, whether you choose to participate or not, I appreciate your consideration of my request, and look forward to meeting you in person.

Warm Regards,

Ed Levy