2012-06

Exploration of Best-Fit Solution for Harbormaster Security Information Sharing Systems.

Ware, James G.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/7428

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPLORATION OF BEST-FIT SOLUTION FOR HARBORMASTER SECURITY INFORMATION SHARING SYSTEMS

by

James G. Ware

June 2012

Thesis Advisor:	Douglas MacKinnon
Second Reader:	Glenn Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
June 2012

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE Exploration of Best-Fit Solution for Harbormaster Security Information Sharing Systems.

5. FUNDING NUMBERS

6. AUTHOR(S) James G. Ware

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ______N/A______.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words) In the wake of the attack of 9/11, the United States government recognized that the manner in which threats and information were conveyed was extremely inefficient, and in many cases completely nonfunctional due to disparate data failing to become accurately coalesced. This is especially true within the area of intermodal cargo shipping. Our research explores and seeks to inform the development of requirements for an information sharing system amongst harbor cargo operators engaged in intermodal shipping. Through interviews conducted of MIST's federal and local partners, careful examination of existing MIST findings, and research into best practices in information system design, we seek to provide an analysis of current needs and recommendations for improvements to communications about threats to intermodal shipping. Our qualitative findings, found through interviewing communication systems operators and users, indicate that the generalized lack of trust has created limits to communication that have manifested themselves in different electronic solutions that appear to have been developed without direct input from operators. We also find that there exist overland enterprises (e.g., trucking industry) that lack motivation to provide funding for improved communications infrastructure. Future research efforts may include further identification of communication barriers (e.g., cost) to improve shared communications systems.

14. SUBJECT TERMS Intermodal Shipping, Information Sharing, Harbor Security, Multimodal Information Sharing Task Force MIST, Inter Agency Communications Center

15. NUMBER OF PAGES
105

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UU

THIS PAGE INTENTIONALLY LEFT BLANK

EXPLORATION OF BEST-FIT SOLUTION FOR HARBORMASTER SECURITY INFORMATION SHARING SYSTEMS

James G. Ware
Lieutenant, United States Coast Guard
B.S., Excelsior College, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: James G. Ware

Approved by: Dr. Douglas MacKinnon
Thesis Advisor

Glenn Cook
Second Reader

Dr. Daniel Boger
Chair, Department of Information Systems

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the wake of the attack of 9/11, the United States government recognized that the manner in which threats and information were conveyed was extremely inefficient, and in many cases completely nonfunctional due to disparate data failing to become accurately coalesced. This is especially true within the area of intermodal cargo shipping. Our research explores and seeks to inform the development of requirements for an information-sharing system amongst harbor cargo operators engaged in intermodal shipping. Through interviews conducted of MIST's federal and local partners, careful examination of existing MIST findings, and research into best practices in information system design, we seek to provide an analysis of current needs and recommendations for improvements to communications about threats to intermodal shipping. Our qualitative findings, found through interviewing communication systems operators and users, indicate that the generalized lack of trust has created limits to communication that have manifested themselves in different electronic solutions that appear to have been developed without direct input from operators. We also find that there exist overland enterprises (e.g., trucking industry) that lack motivation to provide funding for improved communications infrastructure. Future research efforts may include further identification of communication barriers (e.g., cost) to improve shared communications systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AIM	Automated Identification System
ALMIS	Aviation Logistics Management Information System
AMSC	Area Maritime Security Committee
APAN	All Partners Access Network
BEMS	Boston Emergency Medical Services
BFD	Boston Fire Department
BMTSP	Boston Multi-modal Transportation Security Partnership
BPD	Boston Police Department
BRIC	Boston Regional Intelligence Center
CAC	Common Access Card
C3CEN	Coast Guard Command, Control, and Communication Engineering Center
CBP U.S.	Customs and Border Protection
CFC	Commonwealth Fusion Center
CGBI	Coast Guard Business Intelligence
CI/KR	Critical Infrastructure and Key Resource
COMDT	Commandant of the Coast Guard
C-TPAT	U.S. Customs Trade Partnership Against Terrorism
DHS	U.S. Department of Homeland Security
DMZ	De-Militarized Zone: An area outside the protected boundaries of one’s network
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
ECDIS	Electronic Chart Display and Information System
FAA	U.S. Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GMAII	Global Maritime and Air Intelligence Integration

G-MOC	Government Marine Operations Control
GMISS	Global Maritime Information Sharing Symposium
HHAN	Homeland and Health Alerting Network
ICE	U.S. Immigration and Customs Enforcement
ILSSA	International Lodging Safety and Security Association
IOC	Interagency operation center
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LNG	Liquefied natural gas
MARAD	U.S. Department of Transportation Maritime Administration
MASO	Multi Agency Strike force Operation
MassDOT	Massachusetts Department of Transportations
MBTA	Massachusetts Bay Transit Authority
MDA	Maritime Domain Awareness
MEMA	Massachusetts Emergency Management Agency
MIC	Medical Intelligence Center
MIST	Multimodal Information Sharing Team
MOITI	Massachusetts Office of International Trade & Investment
MPO	Metropolitan Planning Organization
MSA	Major Systems Acquisitions
NEDRIX	Northeast Disaster Recovery Information X-Change
NMCO	National Maritime Domain Awareness Coordination Office
NMIC	National Maritime Intelligence Center
OEM	Boston Mayor’s Office of Emergency Management
POG	Port Operators Group
PT-ISAC	Public Transportation Information Sharing and Analysis Center
PVA	Passenger Vessels Association
RISS	Regional Information Sharing Systems
SAR	Suspicious Activity Reporting
SELC	Systems Engineering Life Cycle

TSA U.S.	Transportation Security Administration
TSSP	Transportation Systems Sector-Specific Plan
TWIC	Transportation Worker Identification Credential
UASI	Urban Area Security Initiative
USCG	U.S. Coast Guard
UCD	User-centered design
VIPR	Visible Intermodal Prevention and Response Teams
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This writing would not have been possible without the tireless efforts of Mrs. Anita Salem and her wonderful insights into what she has revealed to be a wicked problem.

Dr. Douglas Mackinnon’s contribution cannot be overstated in that he never lost faith in my work and provided me the decoder ring for successful thesis writing as well as great personal inspiration to persevere.

Professor Glenn Cook’s polite and persistent guidance kept focus on what was truly important and willingness to pitch in when I would get stuck (every other week.)

The interviewees, who gave so graciously of their time and forgave all of my transgressions as an inexperienced interviewer performing his first interviews.

The greatest contribution to this paper came in the form of my family’s great love for me and faith in the process at the Naval Postgraduate School. I am so thankful to them for putting up with the long nights of writing and rewriting, time away from home conducting interviews, and dealing with me when I expressed just how uncomfortable I am as a writer.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INTRODUCTION

The United States relies heavily upon its sea-lanes to deliver and receive economic goods. Each delivery seaport requires sound and reliable security to ensure the proper handling of these goods. Information sharing structures help protect this critical supply chain. Specifically, there are a number of communication channels that are currently used to support the sharing of threat information in the maritime industry. Two primary channels are face-to-face meetings and websites. However, each of these channels has its limitations.

Face-to-face meetings are an effective means of exchanging threat information and helping stakeholders better understand inner agency workings. However, these activities keep people from their normal duties, and thus limit their productivity and attendance. This challenge is especially present in smaller ports where there is minimal staff. Thus, these meetings often fail to accomplish their objectives when personnel simply cannot attend due to work demands. websites have also been developed to solve information sharing problems by leveraging technology to overcome the barriers of time and place. While many of these websites are proficient in some areas; almost all are of limited utility because of the lack of useful and easy-to-use information. These issues and those arising from the operators' reluctance to use these websites, can be addressed by engaging users and seeking new ideas to help determine best fit architectures to assist in Information Sharing.

In the fall of 2008, the Naval Postgraduate School began the *Multimodal Information Sharing Team (MIST)* to investigate possible improvements to the sharing of threat information in America's ports. MIST conducted local events at ports across the U.S. that included site studies, workshops, and community building activities. MISTs goals are to:

- Identify incentives for sharing threats
- Clarify the needs of the private sector in the sharing of threat information
- Investigate ways to streamline government requests
- Explore solutions that improve local collaboration.

MIST has identified several issues that have limited the sharing of intermodal shipping information. Conventional solutions, such as weekly security meetings for instance, are being employed in the busiest ports and have experienced limited success. Harbor personnel are also somewhat resistant to new technology despite well-meaning websites that still have not provided the information that they need in a way that works for them. Expanding on the on-going research of the Multimodal Information Sharing Team (MIST) at NPS, we will conduct interviews of MIST's federal and local partners to help clarify the specific needs of the Boston maritime shipping community.

Given the challenges in information sharing, this research seeks to better inform the development of requirements for an information sharing system amongst harbor operators. These requirements will seek to leverage existing technologies and meet the specific needs of the maritime community in varied environments.

Future efforts can build on this research by researching the development of information sharing systems that are tightly coupled to diverse roles such as emergency action in the wake of a major catastrophe. In those scenarios, multiple agencies often have a need to coordinate their efforts across information sharing medium with in which individual participants may not have experience. Such research, could further enhance the importance of being able to dynamically scale information sharing to a relevant few users or as many as necessary. Another worst-case scenario presented by disaster relief operations is flexibility to shift information sharing across multiple mediums when one of the avenues of delivery is denied—i.e., no phone coverage, no intranet, nor available equipment, in effected regions.

B. PROBLEM STATEMENT

The United States needs improved information sharing structures in the threat environment of intermodal shipping. This research will help inform the development of requirements for an information sharing system amongst harbor operators engaged in intermodal shipping. Through interviews conducted of MIST's federal and local partners, careful examination of existing MIST findings, and research into best practices in information system design, we seek to provide an analysis of current needs and recommendations for improvements.

C. LITERATURE REVIEW

To support our research, we will review the following topics:

- Background, history, and policy issues relating to the sharing of maritime threat information.
- Recent findings on information sharing needs and gaps in port security
- Best practices in human factors design of information systems

D. RESEARCH QUESTIONS

1. How have mutually exclusive efforts of information sharing services impacted quality of information sharing?
2. How would one of the existing multi service information sharing tools be improved to selectively incorporate information useful to any roles that are involved in harbor operations?
3. How can we understand the effects of replacing face-to-face meetings with the introduction of a technology?
4. How can an information sharing structure be designed that leverages Boston Harbor's findings and be scaled for use by other harbors?

E. RESEARCH METHODS

Our qualitative approach will include a review of existing reports on the sharing of threat information, a literature review of best practices in the design of information systems, and semi-structured interviews of U.S. Coast Guard stakeholders in the Port of Boston. Our interview questions are:

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.

2. What is the method used to design and/or select Command and Control (C2) systems to share information?

   a. What are the procedures, requirements, and decision points that are used?

3. How do requirements for information sharing systems drive training requirement for newly arriving personnel?

4. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?

   a. Ease of use?

   b. Desirability (of wanting to use the system)?

   c. Usefulness?

5. In a perfect world—without any constraints—how might information sharing be improved within the Coast Guard?

F. PROPOSED DATA, OBSERVATION AND ANALYSIS METHODS

Reports will be analyzed for strengths, weaknesses, opportunities, and threats to a sustainable information sharing system. Our literature review will be used to identify key human and strategic factors involved in the design of usable information systems. Interviews will be analyzed to identify specific information sharing needs and challenges. Finally, we will analyze all of the above to create a fit comparison of common criteria anchored in human factors.

G. POTENTIAL BENEFITS, LIMITATIONS AND RECOMMENDATIONS

The potential benefits of this research are that the government will be able to develop common criteria for maritime information sharing that takes into account human factors. These common criteria may provide harbor personnel a structure for future designs. Ultimately, the benefit would come in the form of improved security of harbors. The limitations of this research are the model chosen may be inadequate for certain harbors.

H. CHAPTER OUTLINE

The thesis research and findings will be organized in the following manner:

I. General Information and Introduction

II. Literature Review

III. Methodology

IV. Decomposition of the U.S. Coast Guard’s experiences in information systems design

V. Conclusions and Recommendations for follow on work

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. OVERVIEW OF INFORMATION SHARING SYSTEMS

What is an information sharing system? The DoD defines information sharing as "Making information available to participants (people, processes, or systems) (Grimes, 2007). To this definition, this thesis intensifies the discussion by further adding that the effectiveness of these transmissions can potentially save millions of lives. In 2008, the terrorists that attacked the Taj Mahal and many other spots in Mumbai, India, did so initially from a hijacked fishing vessel, then transferred to a rubber dinghy directly into Mumbai Harbor; thus exploiting India's weak communication system and carrying out one of the most gruesome terror attack in many decades. It was during that same year in November, that MIST stood up at the Naval Postgraduate School. The Multimodal Information Sharing Team "(MIST) engages with government agencies and private sector shipping to improve the sharing of threat information" (Salem, 2011).

MIST looked at several facets of information sharing systems, and what the de-facto standards were for that time. Heavily focused on the directives provided by the 9/11 commissions guidance, their keen insights provide the basis of this thesis, and will be referred to throughout its pages. As of this writing, the most recent publication of MIST, was from its Boston seminar, which also helped to explore many of the questions posed in this thesis. Some interesting results were noted by the researchers with MIST, which will presented here for comparison to what the Coast Guard must balance on a day to day basis.

MIST's key findings, which will be examined in greater depth in Chapter IV were: explorations of motivations, collaborative capacity, and threat information. The seminar experienced a modest turnout as there was a fair amount of competition for participants, but many would chose to try to attend both seminars over the course of the week in November to the benefit of the MIST researchers. By benefit, it is meant that having individuals who may not have otherwise been funded to attend this federally hosted seminar show up brought a unique accent to the Boston's seminar. This thesis will focus on is what made the Coast Guard a stand out and specifically why they stood out.

What appeared to be missing from the research was the question: how did the Coast Guard build trust among port partners to a level that each felt comfortable sharing threat information; while at the same time knowing that they would deploy that information responsibly. Perhaps a more interesting question from the authors' point of view was; what had the Coast Guard gained or lost in the shadow of its much larger parent organization DHS that would enrich the discussion of what future system requirements will be?

MIST's report recognized the Coast Guard several times in a sort of *best in class* type of recognition for essentially garnering the trust of other port partners. So, what is the Coast Guard's Strategy for information sharing? The Coast Guard currently follows parent organization DHS, so some highlight of that strategy will be delineated here, followed by a brief summary of the National strategy for information sharing, and finally, the highlights of the DoD's information sharing strategy will provide some factors for comparison.

The DHS's strategy for information sharing is a very dynamic approach to a very difficult problem and GAO has marked them low for compliance on a number of issues like measures of effectiveness or listing users of the system. One could reasonably make the argument that as it has such a difficult task, the standard time lines cannot be applied to DHS in its efforts. What is very apparent in the language of DHS's information sharing strategy, is that it is still very open ended or non-committal. (Department of Homeland Security, 2011) What DHS has done is rather ingenious, in that this looseness of initial conditions allows defining the environment these systems will operate in and ensures a best fit. Its guiding principles are: fostering information sharing, use the established governance structure, committing sufficient resources to its development, measuring progress toward goals, and finally maintaining information and data security while protecting privacy and civil liberties (U.S. Department of Homeland Security, 2011).

Because of DHS's need to accommodate both public and private sectors that are port partners, their strategy does have many similar policies to those of the National Strategy for Information Sharing (NSIS). The NSIS is the overarching information strategy, which best practices in information exchange between public and private port partners go for guidance on how to best communicate with their neighbors.

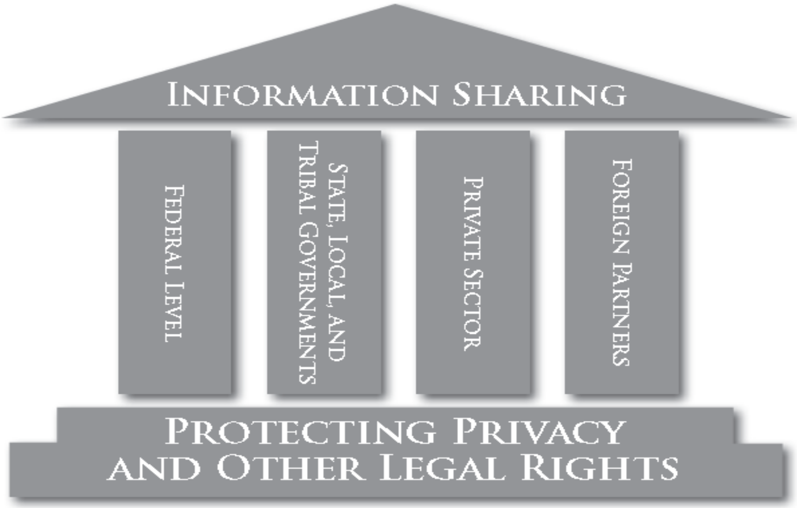

Information Sharing
Federal Level
State, Local, and Tribal Governments
Private Sector
Foreign Partners
Protecting Privacy and Other Legal Rights

Figure 1. Foundations of the National Strategy for Information Sharing (From National Strategy For Information Sharing Successes and Challenges in Improving Terrorism-Related Information Sharing, 2007)

The DoD's information sharing strategy is much more defined than DHS's because DoD has a reasonable expectation that they have fewer stakeholders and none of the real commercial complications that DHS does. DoD's goals as defined in DoD Information Sharing Strategy (Grimes, 2007) and they are clear: promote, encourage, and incentivize sharing, achieve an extended enterprise, strengthen agility, to accommodate unanticipated partners and events, and finally, ensure trust across organizations. Unlike DHS, the DoD also has clearly defined stovepipes to the sharing of information which are: recognize and leverage the information sharing value chain, forge information mobility, make information a force multiplier through sharing, promote a federated information sharing community/environment, and finally, address the economic reality of information sharing (Grimes, 2007).

B. BACKGROUND, HISTORY, AND POLICY ISSUES RELATING TO THE SHARING OF MARITIME THREAT INFORMATION

When John Smith discovered Boston Harbor in 1614 he could not have envisioned what a significant role it would have in the history of the colonies nor its growth into one of the most important harbors in present day intermodal shipping to and from the United States. Boston Harbor is the oldest continually active port in the Western Hemisphere and acts as the maritime hub for all of New England. Some 34,000 people rely on Boston Harbor for their employment and more than eight billion dollars in revenue is introduced into the local, regional, and national economies through indirect, direct, and induced impact (MASSPORT, 2011). Because Boston's busy harbor and close proximity to a major population, supply chain security is of the utmost importance for the Department of Homeland Security which has a relatively large footprint in Boston Harbor as well.

Boston Harbor is part of the larger Massachusetts Harbor, which comprises 50 square miles with 180 miles of shoreline and 34 harbor islands (MASSPORT, 2011). The outer harbor is comprised of three bays to the South East of Logan International Airport; Dorchester, Quincy, and Hingham. There are two deep-water anchorages that are separated by Long Island, which marks the beginning of where the two channels begin. The two channels being, President Roads for the entry point to the Inner Harbor and Nantasket Roads for entry to the Weymouth Back River and the Weir River.

The many associations that operate close to Boston Harbor and are relevant to this thesis are Volpe Center, State Fusion Center, Boston Fusion Center, and the Regional Intel Center. (Salem, 2011) The commercial operators currently operating in Boston Harbor, are a veritable who's who of global shipping giants that include two of the top ten largest in the world; Mediterranean Shipping Company (MSC) and China Ocean

Shipping Company (COSCO). This list also includes FedEx, Delta Airlines, and various other global maritime shipping and local maritime shipping companies.

C. RECENT FINDINGS ON INFORMATION SHARING NEEDS AND GAPS IN PORT SECURITY

Volpe Center is unique in that their vision is "to be the leading federal center of excellence for innovative transportation systems solutions" (Administration, 2011). Volpe Center's mission, which is "To improve the nation's transportation systems" (Administration, 2011) will make them a key reference throughout this thesis. Their strategic goals include: contributing to solving U.S. DOT's key challenges, influencing the direction of the national transportation enterprise, ensuring a sustainable business model, and continuously developing the center's human capital. Volpe Center enjoys a reputation for being entrepreneurial, market driven, and innovative and is consulted regularly by both government and private interests (RITA, 2011).

The Global Justice Information Sharing Initiative defines a fusion Center as "A collaborative effort of two or more agencies who provide resources, expertise and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activities" (Burke, 2007). This is echoed in the State of Massachusetts's fusion centers mission statement:

> The Commonwealth fusion Center collects and analyzes information from all available sources to produce and disseminate actionable intelligence stakeholder to strategic and tactical decision-making in order to disrupt domestic and international terrorism. (Burke, 2007)

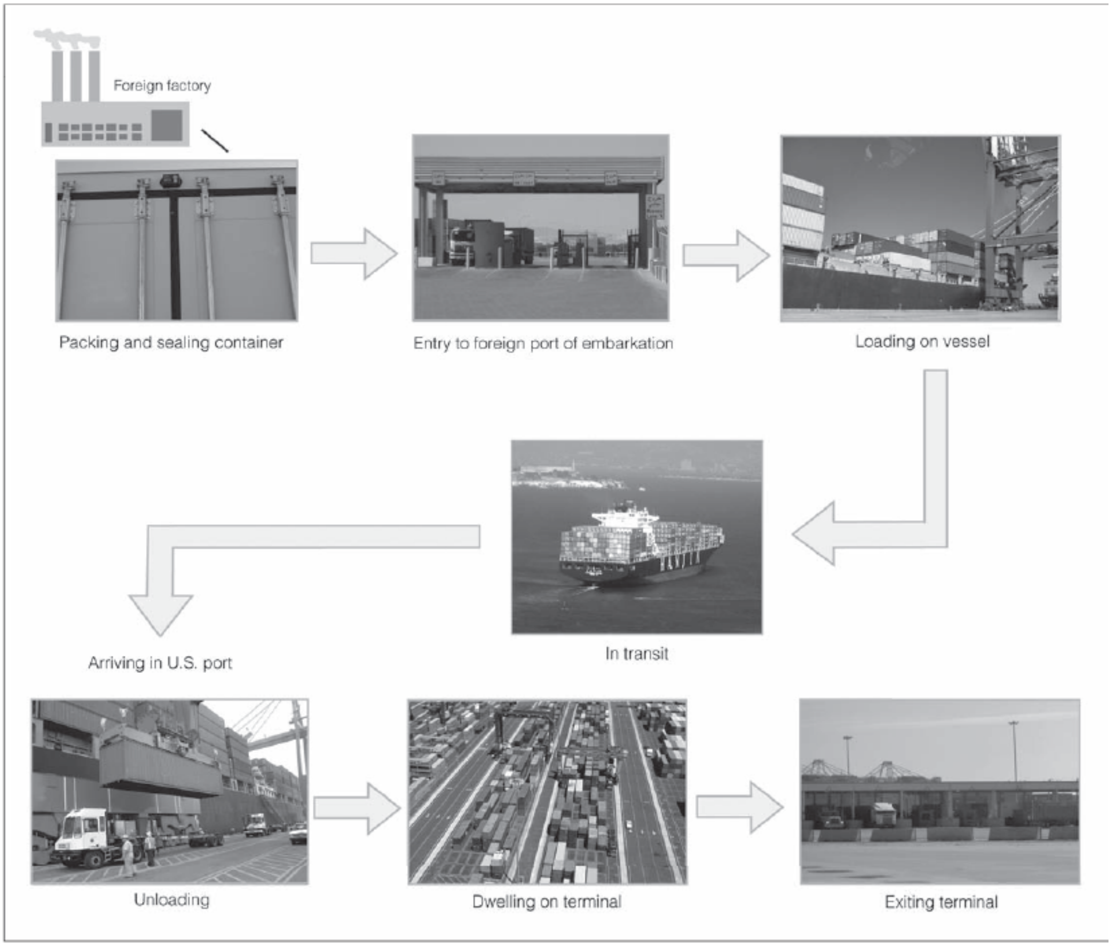
The State of Massachusetts fusion centers goals are as follows: work in partnership with local, state, regional and federal public safety agencies; implement secure, comprehensive mechanism for the timely exchange of information; provide accurate and timely intelligence products; provide direct analytical support for investigations involving precursor criminal activity; and promote awareness of priority intelligence requirements and of indicators of threats to the Commonwealth. (Burke, 2007) The state and Boston's fusion centers generally act as a central repository for information and analysis accessible by almost all law-enforcement agencies that operate within the state of Massachusetts (Burke, 2007). This information is deliverable to these agencies in the form of products that are bulletins, intelligence, and information's briefings and strategic assessments.

Over the years, Boston Harbor has either led the field or been near the top in its efforts to keep pace with technological changes involved in intermodal shipping. Today the character of Terry Malloy played by Marlon Brando in the 1960s movie O*n the Waterfront* would be more likely to carry a clipboard with the day's choreographed movement of containers than anything that would in fact be shipped. The days of the stevedores busily handling large bags of coffee and barrels of oil are long gone and have instead been replaced by enormous gantry cranes capable of lifting in excess of 50,000 pounds (Levinson, 2006). What has triggered these role reversals? The introduction of containerization to the shipping industry by a company in New York named McAllister Trucking. McAllister Trucking had the vision to see that the more times cargo was handled the more expensive the process was (Levinson, 2006). This realization revolutionized the shipping industry from the ports that handled the containers, the ships that moved the containers, to the supply chains that developed because of the containers. On any given day, the port of Boston is buzzing with activity; gantry cranes lift stacks of 40 foot long containers out of the lower holds of the enormous oceangoing container ships onto waiting trucks where they can be halfway across the state and on local warehouses that same day.

In South Boston, Massport's Paul W. Conley container terminal sits on 500 acres of waterfront property, and handles close to 1.5 million metric tons of cargo each year. Some of the top containerized imports include beer and wine, frozen seafood, furniture, footwear, and toys. The chief exports are paper, which includes wastepaper, scrap metal, autos, skins, hides, logs and lumber (MASSPORT, 2011). Perhaps more interesting and certainly more relevant to this thesis is what the Port of Boston handles as containerized and bulk; 15 Million metric tons of which include petroleum, natural gas, gypsum, and salt. These cargoes are a small concern; however, when positioned in close proximity to large populations, the cargoes become valuable terrorist targets. It is for these reasons that the port of Boston has one of the best-established information sharing systems in current usage in the country.

Like many of the other harbors within the United States, Boston, because of the sheer volume of containers that are handled there, is a likely target to not only venders for movement of goods, but terrorists for movement of weapons as well (Salem, 2011). Indeed, Boston's major population, adjacent to Conley Terminal, where containers are unloaded and loaded daily, presents its own set of unique challenges. "This high-efficiency transportation machine is a blessing for exporters and importers, but it has become a curse for customs inspectors and security officials" (Levinson, 2006). The threat surface, when discussing supply chain type vectors, has to take into account the factors depicted in Figure 2.

Boston Harbor may be ideally suited to test potential solutions to these threats because of its tight-knit maritime community. However, with so many stakeholders and so much at stake, the DHS has a difficult task if they wish to come up with a lasting solution to this persistent problem (Grillot, 2010).



Source: GAO (analysis); GAO and DHS S&T (photos).

Figure 2. Container Movement. (From United States. Government Accountability Office, 2010c)

As of September 2010, there were four competing technologies to help alleviate the problem, those technologies are listed in Table 1. DHS should test and evaluate container security technologies consistent with all identified operational scenarios to ensure the technologies will function as intended": (Government Accountability Office, 2010c) The GAO's report indicated that DHS needed to test containers on parameters that would be consistent with all threats. This difficult task was complicated by the fact that the containers are the perfect vessel to intermodal transport of goods. To overlay security requirements onto a highly lucrative business is not without controversies.

Description of DHS S&T's Four Container Security Projects Project name	**Project description and goal**
Advanced Container Security Device (ACSD)	Develop a device that can detect and report container intrusion on all six sides of a container.
Container Security Standards and Devices (CSD)	Develop a device that can detect and report the opening or removal of container doors.
Hybrid Composite Container (HCC)	Develop a composite container with embedded security sensors to detect intrusion on all six sides.
Marine Asset Tracking Tag System (MATTS)	Establish a system to track containers, and increase the range that CSDs and ACSDs can communicate.

Source: GAO analysis of DHS S&T information.

Table 1. Competing Technologies

All technological solutions in Table 1 attempt to ensure that any unauthorized or undocumented opening can be easily detected. However, all of these solutions are still only as good as the humans who maintain them. Thus, the problem moves back to a neuron's solution as opposed to an electron solution which demands a stronger focus on information flows, incentives to cooperation between stakeholders, and a thorough analysis of information desirability.

As one of the organizations that has traditionally been charged with upholding federal policies, the Coast Guard has been viewed by its port partners as an organization that takes a pragmatic approach to their implementations. In this capacity, the organization struggles to strike the proper balance between those same partners and upholding the law. However, as reflected in the interview with the (Operator, 2011), there has been a host of new laws pushed down on the Coast Guard to enforce and there is also a tremendous amount of overlap of these policies which only confuses port partners. As the Coast Guard calls into question some of the newer laws, they become increasingly busy dealing with a population that has grown weary of any new mandates and in effect lost faith in the Coast Guard as a trusted partner further pushing the federal government out of the day to day workings of the harbors it seeks to control.

D. BEST PRACTICES IN HUMAN FACTORS DESIGN OF INFORMATION SYSTEMS

Another ramification of 9/11 was that the U.S. government struggled to improve the sharing of threat information amongst all communities that were to be working together underneath Homeland Security. Most notably among the mandates that were passed by Congress was the U.S. Patriot Act, which was designed to ensure there would be no obstructions between criminal investigations and intelligence operations. This however was a smaller effort then the presidential executive order 13228, which saddled DHS with fixing the fragmented information systems that predated that department. The current state of information flow in Boston may be aptly characterized as fragmented and very complex, and yet it is through this adversity that Boston Harbor has emerged as one of the best examples of human systems filling in the gaps that are either created or left from multiple communication systems that had been developed exclusively from one another.

Adding to the challenges offered in Boston Harbor, are its sizeable population in close proximity to the Harbor. It is a shared space with one of the busier airports in all of the United States, and the fact that so many agencies are responsible for overseeing an extremely robust commercial operational environment make things difficult as well. This thesis will highlight the unique approach that the United States Coast Guard has employed which has earned it high marks by all entities in both Boston Harbor and throughout the ports in which they have a role.

The stakeholder’s organizations in Boston Harbor that support information sharing of some kind are presented here in four lists: private sector, regional and state, city, and federal organizations: This list is not meant to be exhaustive, but provides a survey of regional resources available for sharing multimodal security threat information.

E. PUBLIC-SECTOR RESOURCES

1. State Resources

Boston Emergency Medical Services (BEMS) Has the responsibility of providing emergency medical services within the City of Boston (City of Boston, 2012).

Boston EMS Medical Intelligence Center (MIC) To connect Boston's EMS to the public and private entities responsible for first response, hospital services, and public health and safety the Stephen M. Lawlor Medical Intelligence Center Boston EMS also works within the Boston Regional Intelligence Center (BRIC) to stay informed (City of Boston, 2012).

Boston Fire Department (BFD) Upholds their commitment to serving the community by protecting life, property and the environment utilizing some 467 uniformed personnel and managing two Divisions and eleven districts. (City of Boston, 2012)

Boston Mayor's Office of Emergency Management (OEM) Enhances the City of Boston and Metro-Boston Homeland Security Region's (MBHSR) capacity to prevent, protect against, respond to, and recover from major emergencies. (City of Boston, 2012)

Boston Police Department (BPD) Partnering with the community of Boston to improve citizen quality of life by fighting crime, and reducing the fear of crime (City of Boston, 2012).

Boston Regional Intelligence Center (BRIC) Gathers and analyzes intelligence to inform BPD tactical strategies. Intelligence is focused on mitigating threats related to organized crime, terrorism, or individual acts of violence. Actionable intelligence related to threat information is shared with local stakeholders to prepare and respond to threat incidents. (Salem, 2011)

Commonwealth Fusion Center (CFC) Information aggregator aimed at disrupting international terrorism. (Commonwealth of Massachusetts, 2012c)

Massachusetts Emergency Management Agency (MEMA) Responsible for the state's resilience to disaster (Commonwealth of Massachusetts, 2012b)

Massachusetts State Police Responsible for providing policing activities for the public safety inclusive of roadway trafficking, crime reduction, and patrol services for critical incidents (Commonwealth of Massachusetts, 2012e)

U.S. Coast Guard Sector Boston Responsible for container, domestic vessel, and facility inspections, waterway management, port control, and homeland security investigations duties within the Boston Harbor area (U.S. Department of Homeland Security, n.d.).

Volpe Center Mission is to improve the Nation's transportation system. Their work is performed for U.S. DOT, as well as other Federal, state, local, and international agencies and entities (RITA, n.d.).

2. Federal Resources

U.S. Coast Guard National Headquarters Protects the maritime economy and the environment, defends our maritime borders, and saves those in peril at sea (U.S. Department of Homeland Security, 2012, May 16).

United States Coast Guard Interagency Operations Center (IOC) The IOC framework enables a unified coalition of port agencies to conduct and apply risk-based operational planning for efficient, collaborative use of multi-agency resources for improved operational effectiveness (U.S. Department of Homeland Security, 2012).

U.S. Customs and Border Patrol (CBP) Mission is keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws (U.S. Department of Homeland Security., 2012).

U.S. Department of Homeland Security (DHS) To prevent, to protect, to respond, and to recover, as well as to build in security, to ensure resilience, and to facilitate customs and exchange (U.S. Department of Homeland Security., 2012).

U.S. Department of Transportation (DOT) Serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future (United States Department of Transportation, 2012, March 27).

Department of Transportation Maritime Administration (DOT – MARAD) Improve and strengthen the U.S. marine transportation system to meet the economic, environmental and security needs of the Nation. (U.S. Department of Transportation Maritime Administration, 2012)

Federal Aviation Administration (FAA) Our continuing mission is to provide the safest, most efficient aerospace system in the world (Federal Aviation Administration, 2012).

Federal Bureau of Investigation (FBI) As an intelligence-driven and a threat-focused national security and law enforcement organization, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners (FBI.gov, n.d.a).

Federal Bureau of Investigation Joint Terrorism Task Force (JTTF) Boston The nation's front line on terrorism: small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies (FBI.gov, n.d. b).

Federal Emergency Management Agency (FEMA) Support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards (U.S. Department of Homeland Security, 2012 Mar 13).

Information Sharing Environment (ISE) Provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep our people safe (ISE.Information Sharing Environment, n.d.).

U.S. Immigration and Customs Enforcement (ICE) Promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration (U.S. Department of Homeland Security, n.d. c).

National Maritime Intelligence Center (NMIC) Protect the United States from hostile and illegal threats in or emanating from the Maritime Domain, by ensuring that intelligence is fully integrated in support of national policy and operational decisions (National Maritime Intelligence-Integration Office, n.d.).

National Maritime Domain Awareness Coordination Office (NMCO) Facilitate the creation of a collaborative global, maritime, information sharing environment through unity of effort across entities with maritime interests. In order to achieve Global Maritime Situational Awareness, we must increase the discoverability and share-ability of information relevant to those engaged in managing the security, safety, environment and commerce associated with the maritime domain (National Maritime Domain Awareness Coordination Office, 2010).

Transportation Security Administration (TSA) Protects the Nation's transportation systems to ensure freedom of movement for people and commerce (U.S. Department of Homeland Security, 2012 b).

Transportation Security Administration Freedom Center Formerly the Transportation Security Operations Center (TSOC), the Transportation Security Administration Freedom Center in Herndon, VA, coordinates real-time intelligence sharing in response to security incidents and operations related of transportation networks. The Freedom Center acts as an operational intelligence hub to mitigate security threats in conjunction with the Federal Air Marshal Service, Federal Aviation Administration, Department of Defense, and other federal agencies tasked with homeland security responsibilities (Salem, 2011).

F. PRIVATE-SECTOR RESOURCES

Boston Harbor Pilot Association, LLC The Boston Harbor Pilot Association is composed of Massachusetts's state-commissioned pilots who operate vessels entering and departing the Port of Boston. They are the only state and federal pilotage service that operates 24/7, and their goal is to maintain environmental stewardship of the Boston Harbor while ensuring the safe free flow of commerce through maintaining security and acting in the public interest (Salem, 2011).

Massport Owns and operates an integrated world-class transportation network that promotes economic growth and opportunity, enhances the quality of life of New England residents and protects the freedom to travel safely, securely, efficiently and cost-effectively. Strives to always be a good steward by treating colleagues and customers with respect, embracing diversity and minimizing the impact of transportation services on our neighbors and the environment (Massport, 2012).

Northeast Disaster Recovery Information X-Change (NEDRIX) Provides continuity and crisis management professionals' access to real time governmental agencies information during a crisis or event (Nedrix, 2012).

Passenger Vessels Association (PVA) Focuses on the issues and concerns most relevant to owners and operators of passenger vessels, manufacturers of maritime-related products and services and other service companies dedicated to achieving a common goal...working to develop a superior business environment for all (Passenger Vessel Association, 2007).

Public Transportation Information Sharing and Analysis Center To strengthen and improve public transportation, APTA serves and leads its diverse membership through advocacy, innovation and information sharing. APTA and its members and staff work to ensure that public transportation is available and accessible for all Americans in communities across the country (American Public Transportation Association, 2012).

A *common sense* approach was desperately needed if progress was to be made in streamlining communications; especially in regards to threat sharing. It was determined early on, that the collaboration would be instrumental in this effort. The problem was approached from the standpoint of, what could be done from traditional methodologies (not employing technology) that enhanced that collaboration.

Weekly Group meetings called Port Operators Group Meetings are the de facto standard that has been the bulwark for Boston Harbors' collaborative success. In the MIST Boston Report, it was the consensus amongst stakeholders that meetings were effective as long they were somewhat narrowly focused. Also of value from these meetings are text contacts and calling lists with people that trust each other and have contexts for how they react to different situations. It is this trust that has elevated the Coast Guard into its pivotal role in shaping the way an information system/threat sharing should work. The Coast Guard, as it works with the commercial sector every day, has aligned itself to enhance commercial capabilities while at the same time focusing on security concerns; two factors that are often diametrically opposed.

Having reviewed three information sharing systems, a history of Boston Harbor was presented that highlighted the background with which thesis discussions will be grounded. Particular focus on what the DHS has in common with the other information sharing systems comparison will continue to give rise to the questions, which will be laid out in Chapter III. The non-exhaustive list of interests that will be impacted by any future information sharing system was presented to further define the landscape of possible consideration of alternative demands that will be placed upon it.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. INITIAL CONDITIONS

Port security has been a mission for the Coast Guard for much longer than it has been a hotly disputed international issue. Presently, the Coast Guard relies heavily on its reserve forces for port security, and they are highly skilled in its methodologies. Internationally, Israel is amongst the best in the business and could be considered battle hardened after their fuel and chemical tanks narrowly missed being ignited in 2004. “On March 14, two suicide bombers breached port security by hiding behind a fake walls placed in freight containers.” (Grillot, 2010) This passage was placed here to indicate the level of commitment of today’s adversaries. Had this same scenario been played out at one of the fuel treatment plants at Conley terminal in the Port of Boston, there would be hundreds if not thousands of casualties.

MIST’s fifth seminar offered the ideal opportunity for the author to meet face to face with many of the individuals representing the stakeholders outlined in Chapter II. However, due to unforeseen financial complications in days leading up to that seminar, travel would not be possible. It was during this time, however, that a most optimal path was presented for research to the author. The Subject Matter Specialist offered research into what the Coast Guard was doing correctly to earn trust of its port partners in Boston and at all other ports for that matter. The Subject Matter Specialist obviously had a vested interest in determining that information as it would fuel the discussion of best practices of organizations to build systems that may be employed in the near future for conveying threats.

Of the key findings observed by MIST; motivations were found to “energize human behavior and should be addressed when planning for the sharing of threat information.” (Salem, 2011) Collaborative capacity is “the capability of organizations to build the institutional mechanisms that support collaboration.” (Salem, 2011) One of the better known issues that was “threat information needs to be readily accessible and relevant" (Salem, 2011). A fact, which was also echoed in the 9/11 commissions report. Finally, what the author found to be most inspiring, "local models for information sharing can help other ports learn best practices" (Salem, 2011). One of the more specific findings cited in the MIST report from the 2011 seminar in Boston had also been captured in one form or another in every other seminar which MIST had conducted was "Private sector participants want to collaborate and share information but a number of barriers inhibit that collaboration." (Salem, 2011) It was also pointed out in that report, that as promoting and protecting the commerce, the Coast Guard has done an excellent job aligning itself with commercial goals. That alignment enhances the trust required for information to flow without fear of compromising proprietary information. It was from the realization that the following research questions were developed to depict lessons learned through trial and error of the Coast Guard.

The first task in seeking answers to these research questions was to prune a list of who is who within the Coast Guard, which could characterize why an organization has been successful in establishing trust. To answer the research questions, suitable interview questions were constructed and vetted for relevance to the main questions. Those questions listed here when answered by the individuals that were in the meetings where policies were set or systems chosen will provide a best-fit solution to the overall research questions as well as many valuable lessons learned.

B. WHAT IS THE BROAD MEANING OF PORT SECURITY?

Just as the name implies, port security is the security posture experienced by a port relative to verifiable threats both natural and manmade. To cite a best in class for port security, as was indicated previously, Israel has hardened it's harbors and even the incident previously illustrated, had it not been for swiftly moving security forces at the time, the number of dead could have easily went from sixteen to a few thousand. Having had experience with physical security on military instillations, there usually is no substitute for *Guards, Guns, and Gates*. Therefore, when trying to project ones thinking from the traditional neuron solution to one utilizing electrons, it is useful to keep in mind that it is essentially changing peoples mindsets to reflect how future attacks may occur. A subtle point being, to move too fast is to create a system that only a small number of port partners would use. Yet, in going too slow, advisories that are historically much faster at adapting new technologies to their purpose will capitalize on its new found utility to render *slow to field* solution untenable.

There are a number of remarkable information sharing systems which are already in place like Homeport, the All Partners Access Network (APAN), and the Maritime Domain Awareness Information Portal to name a few. What are these systems lacking? In short, it is customer buy in. As MIST had pointed out, there is one of a handful of factors, which render these complex solutions untenable. Depending on which system one choses, symptoms range from no security on some, to dated information on another and flat out useless information on others. Different password renewal processes hamper a good number of all of them, however, one factor stood out to this researcher, which was the lack of trust in one system to do everything. This lack of trust was mostly rooted in personal experience which may or may not reflect the current state of any system but it none the less rules out many of them. This means that systems have essentially ended up right back where they started and not solved anything. Thus, the far more interesting question to this researcher was just how endemic this lack of trust was only to have it confirmed by MIST that there is in-deed a tremendous amount of mistrust amongst port partners. Again, what set Boston apart from other ports that suffer similar lack of trust is that they have instituted weekly face-to-face meetings. Although this is an effective fix for the time being, it does not scale to all harbors and creates other problems, which are beyond the scope of this thesis.

C. OVERALL RESEARCH DESIGN

A qualitative approach was chosen for this research, as initially very little was understood about the general history of the Coast Guard build process for new systems, and only a tacit and vague understanding of it port policies were available. A case study strategy was utilized with the hope that pre-9/11 methods would be somewhat varied from sample to sample and would combine to form an overall picture. It was decided early on in the process that semi-unstructured interviews of purposeful samples would offer the best cross section of individuals who had an input into making the Coast Guard into the agency that had earned the coveted trust.

A proposal was drafted and approved in mid-August 2011 and exists as the introduction chapter of this thesis. The IRB process was rigorously adhered to and an approval for questions was granted in the first days of September.

As far as performing these interviews practically, it was also decided that the listing of samples had to be constructed using as much insider information as possible. This would assure that there would be true organizational type barriers that had to be overcome in order to be successful. More to the point, as a researcher, what was far more constructive, were the elements that did not work or could be improved upon to provide added utility to future systems developers. An initial contact was offered by the MIST Subject Matter Specialist for someone who was actively participating in the port security process in the Boston area (Operator) that was where the list started. For the next sample, the author used prior knowledge of individuals who were in the role of (System Manager) to offer their view of the process as cultivated during their watch. From those first two valuable contacts, the other two (Designers) were obtained for interview as well. Finally, a person who was actively making design decisions for the Coast Guard and who had signed the initial RFP for the systems that the Coast Guard currently relies on (the technical director) was solicited for background and future direction.

Interviews began September 9, 2011, with the first one taking place over the phone with digital recording equipment. As the interviewee was located in Boston, the time change had to be factored in as it would also have to be in every single one of the interviews that were to be carried out at that time. This particular interviewee was particularly helpful as this had been the subject of his own personnel inquiry for several years and he proved to be most insightful in his role as the operator.

The second interview took place on October 18th, 2011 in a similar fashion using digital recording equipment. The second interview was flavored quite differently than the first however, in that the author had personally worked for this interviewee before and from memory recalled that the individual had experience with Rescue21 for the Coast Guard, which made him the ideal system manager. This particular individual was able to refresh the interviewer’s memory on who it was that would be the ideal (Technical Director) for the purposes of this thesis.

On October 28, 2011, ten days after the interview with the system manager, the interview with the technical director took place with a digital recording device. This particular interviewee had a tremendous amount of enterprise data that could not be obtained from the Coast Guard’s Yearly Congressional recordings for that period. This interviewee was most interested in the findings of this thesis and will be on the distribution list with a follow up phone call for feedback.

On November 8, 2011, ten days after the technical director interview, the fourth interview took place. This interviewee would be an ideal designer and offered extensive opinions on everything from what had gone wrong to what direction the Coast Guard would be moving in with its present systems.

It was not until the day after Christmas that the final interview took place. Immediately, it was a different style interview in that the interviewee provided the interviewer with the range of their knowledge so that we were able to make the most of the hour-long interview. What pervaded the interview from the interviewer perspective was the sense that this would be the final interview. Question themes were easily recalled without looking at notes and a risk of embellishing the final product by getting too granular was a real risk.

From an early stage in the interview phase, it was decided that whatever the transcription process turned out to be, a system of member checking to ensure that there would not be any misquoting was utilized. To accomplish this the author, (after initial transcription was carried out), a formal letter was drafted and submitted along with the electronic copy of the individual transcriptions, was sent back to all five of the interviewees. Four of the five made corrections with the fifth being a former supervisor of the author, simply offered that he trusted the interviewer (in an e-mail) to have done a good job translating his remarks.

In keeping with the mandate of the IRB findings the following questions and probes were put forth to interviewees:

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.
2. What is the method used to design and/or select Command and Control (C2) systems to share information?
    a. What are the procedures, requirements, and decision points that are used?
3. How do requirements for information sharing systems drive training requirement for newly arriving personnel?
4. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?
    a. Ease of use?
    b. Desirability (of wanting to use the system)?
    c. Usefulness?
5. In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?

In Section E the author will arrange the questions with a summarization of respondents answers to those questions. Appendix A offers mind maps these interview questions relative to individual points to the questions, also for the readers benefit; whereas, Appendix B is the transcribed interviews of each respondent one through five.

D. CONFLICTION

The main examples of conflict came from the designers. Designer one felt that the quality of training that was taking place at units was adequate. By designer two’s recollection, the training that was offered when a system was rolled out was little more than button ology that did not cover anything beyond the most simple failure of any system and completely lacked realism.

Another incident that conflicted with overall study findings was also provided by Designer two in her experience in the western rivers seminar in which she was approached by a captain of a river-tending vessel. That particular captain indicated when he or any of his coworkers observed something as serious as a buoy being off station, reported that to the Coast Guard, nothing would happen for weeks. A simple technological solution was also offered by Designer two of updating an electronic map tool that all used with a note feature so that when something of that magnitude occurred, the party that reported it could see that it was not simply forgotten. As a researcher who had been immersed in the technologies that had failed because nobody was willing to use them for one reason or another, her proposal ran afoul of many others. In retrospect, her offering would likely work for a short period of time, whereas, a broader solution would last much longer and would in all likelihood scale to smaller rivers better.

This next section illustrates possible connection of points between interviewees and findings. Patterns will be highlighted and analyzed for relevance to each interview question. Followed by an analysis of where the comparisons moved the direction of the author in forming ideas.

E. COMPARISON

1. "As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information."

For the first interview question there was a view that was common to four of the five interviewees that of access to data. From the technical director's point of view, better forms of encryption was where the emphasis needed to be placed. This is in contrast to the view of the operator, whose concern was with who they should be able to share information with in the first place. Designer one also spoke to conflicting firewall requirements limiting access and designer two of more physical issues like bandwidth allocation and turf problems.

The operator had indicated that often, classification of information was a challenge that would confuse watch standers and cause them to hesitate when they needed to get information out quickly. Further complicating this issue was the abundance of regulations that needed to be weighed, before making classification decisions. It appeared that the system manager had a similar opinion in that operators struggled to organize information into functional areas. This is often a challenge within the Coast Guard, as smaller operational units happen upon a situation and are forced to quickly make a decision as to how its transmittal should be accomplished.

The technical director had an interesting take on information sharing in general, in that he indicated that information was not the problem. He cited his experience into past Coast Guard programs that led him to believe that technology had to be the final solution, which did not really resonate with the group as a whole. The technology director even listed a technology, which was being used by SPAWAR called crypto binding offering cradle to grave encryption of data. Probably the greatest contrast to that point of view would be offered in question three by designer two where she indicated that Coast Guards tendency develop a new system then throw it over the wall to see how it was received.

2. “What is the method used to design and/or select Command and Control (C2) systems to share information?

    a. What are the procedures, requirements, and decision points that are used?”

For the second interview question designer one offered a few phases of the Systems Engineering Life Cycle (SELC) and a sort of iterative development. One fact that caught the researcher off guard was that systems were typically not tested on inexperienced personnel due to their complexity. The operator was unable to speak to this question, as he had not participated in the building of any of these systems, only their employment. Designer two was somewhat unsure if there was a method, but she was very candid in indicating how the Coast Guard gets into a big hurry whenever there are monies available and a desire to have a capability often to their detriment. She also indicated that many of the systems that look good on paper do not have any studies done to indicate if the average Coast Guard operations center can handle their added workload. This led to her next point, that anytime a system comes up that may be of use it has to be approached from the standpoint of having no people to operate a terminal.

The technical director decomposed both the Major Systems Acquisitions MSA manual and DHS's SELC and offered that the best takeaway was that sponsors had to stay engaged in the process no matter what the system. This highlights the difference in perspective between designers and system administrators, with one indicating designers panic to get things fielded when there is money available to how admirals must often stand up and ask the "what for?" question. The technical director also pointed out the relative success the Navy had experienced employing user juries in their designs, however this is often too cost prohibitive for the Coast Guard to attempt.

3. "How do requirements for information sharing systems drive training requirement for newly arriving personnel?"

For question three, designer one spoke to smaller technologies being vetted in one particular manner and COTS being used for smaller problems. The operator was not able to speak to this question either. Designer two was again perfectly candid in that "They should be driving at training, but they are not" (Designer two, 2012). What commands were getting back was pretty much simple button pushing skills to their personnel. More specifically, she felt that there was a systemic failure to contextualize training with realistic operational scenarios making real failures that much more catastrophic.

The System Manager diagramed the roadshow methodology that was often employed in place of classroom training and highlighted a common scene of a student bringing up an issue in which a capability should be offered in a system to trainers. The reality of road shows is that even if trainers could force the issue up the chain, by the time it could be implemented the whole system would be obsolete. Another problem that happens all too often is when the Coast Guard does get the green light to install a system, they have such a small window of time that they have to draft the training requirements from the system actually being operational. As designer one pointed out, many of these systems that they test are simply too large and complex to bring to an operational unit and obtain what real watch standers may have to contend with to get a system fielded.

4. “With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?
    a. Ease of use?
    b. Desirability (of wanting to use the system)?
    c. Usefulness?”

Question four had the most commonality of responses in that four of the five interviewees indicated that human factors are highly considered in today’s system.

This commonality of response, avoided the interviewers question purpose which was determining the amount of emphasis designers had put into present systems in common usage within the Coast Guard. Designer Two appeared to understand more of what the interviewer was looking for, when she delivered her answer of “not too much!” She did also indicate that the Coast Guard has since the Rescue21 and others had gone all the way toward human factors with its designs. She also offered an excellent characterization of the problem from her personnel experience with Rescue21 in which a controller at a terminal had to execute 21 button pushes to get time critical, possibly lifesaving information to an operator. Exhibiting the firsthand experience that was so crucial to the overarching purpose of this thesis and triggering a review of all other interviews for references to Rescue21.

The system manager, indicated that all new systems need to be of the “one or two clicks” type to get something accomplished. Which one could reasonably conclude was a product of the Coast Guard rethinking its approach to new build type systems after Recue21 was forced to be recast due to its difficultly of use. This is also indicative that the Coast Guard has truly learned a valuable lesson to start from what the average Coast Guard unit is able to handle for added workloads. There was plenty of support for this from both the operators interview and Designer two both indicating that the average watch stander was maintaining watch over at least four different communications databases.

5. “In a perfect world—without any constraints—how might information sharing be improved within the Coast Guard?”

Question five was designed to be an open forum question and interviewees were invited be very candid and all were very willing to oblige. The technical director indicated several times that the trust the Coast Guard enjoys, is mostly due to the great lengths it goes to handle information in accordance within originators intent. He also highlighted how a policy group that he had chaired for three years failed to come up with a viable solution to the encryption problem but he was convinced it had to be a technological one. There was also a reference to how the FAA assigns numbers to systems based on statistical methods and how that was extrapolated to system costs. He concluded his interview by indicating that the NSA certification of any system that is settled on would mean success.

In response to question five, designer one indicated a departure from the one computer mentality was necessary for designers to get to the next level of systems. Single log in to all systems would cure many of the access issues outlined in question one. “We need to get past the sharing of log-ins and into the sharing of information” (Designer One, 2011)

The operator view of question five was one of reducing the number of mandates that are out there into a single coherent set of rules that all can agree to is the first step. He went on to indicate that some of the policies of late, are indicative of what has been taking place for years, and is often delineated by three other sources. The “single point mooring” (Operator, 2011) type approach needs to be realized within the next few years in order to move beyond the trust that the Coast Guard enjoys to an organization that all commercial partners come to because information sharing has been implemented correctly. The operator also offered an observation that many of the command centers are broken due to turf wars that was later echoed by designer two in her response to question 1. Next, the operator offered whatever system is settled on, there needs to be concern for a single point of failure as well as the buy in because that has plagued many systems as well. He also offered that the ALMIS system was kind of a stand out in pushing information to those it would be relevant to although it did not have the dynamic nature of systems with a sense of place.

Designer two was of the opinion that solutions would come from discussion of agency needs and that at the end of the day work load issues absolutely hamper the USCGs effectiveness. ECDIS (electronic chart) was her favorite for systems that would solve many of the information sharing problems. Finally, she indicated that when the subjects of a system notify of a condition, those subjects need to know what will be done and when it will be done.

The system manager offered three points: 1.) holding people accountable for their actions, 2.) improving governance of systems, and 3.) focusing more on knowledge flows and enforcing standardization. Indeed these are the tenants of any strong system and are truly a reflection of this individual’s knowledge in what makes a system work from a managerial standpoint.

The initial conditions summarized the backdrop of environments that this thesis will draw from. This summary included definitions of port security as well as a brief overview of what MIST’s Boston Seminar would contribute to include its key findings from that seminar. All thesis questions were laid out, followed by operational descriptions of information systems in common usage for comparison. The overall research design was briefly discussed which included broad descriptions of interview logistics concluding with a list of interview questions. A section was devoted to the contrasts and comparisons, that resonated with the interviewer. Overall, this chapter was dedicated to the interviews, which amounted to about 40% of the findings in Chapter V and will be decomposed against overall research questions in Chapter IV.

IV. DECOMPOSITION OF COAST GUARD EXPERIENCES IN INFORMATION SYSTEMS DESIGN

The intent in this chapter is to draw answers to main thesis questions from the interview questions that were asked and summarized in Chapter III. This should provide the connective responses to inform the conclusions of Chapter V. This will be accomplished by reintroducing the questions, then elucidating the themes that came up over the course of interviews and discussions with MIST members to the level that it would be considered in answering the questions. These themes, will also be punctuated with observations of MIST and their findings from multiple seminars.

A. How have mutually exclusive efforts of information sharing services affected quality of information sharing?

When the author originally drafted this question, the hope was that differences and similarities would point to one particular system over another as being a sort of best in class. Interviewees were quick to point out weaknesses of existing systems, but many of the state properties of the systems came from discussion with the Subject Matter Specialist and MISTs interviews with the Operators/ System Administrators.

Systems raised "in a vacuum"

Of the systems mentioned in the interviews, to meet a particular agencies needs in the port environment are becoming obvious in what their limitations are. As MIST had documented in their Boston seminar, the factors, which determine that utility, are Usefulness, Desirability, and Usability (Salem, 2011). One of these systems MARVIEW was developed by the U.S. Department of Transportation Maritime Administration is wonderful for all three factors to the MTS. But when viewed from the lense of the Coast Guard or BPD it does not rise to the level that either service would be willing to put their investment into it.

Another system that was designed for the Coast Guard as its enterprise Internet portal is HOMEPORT, which has been a realitively effective tool as mentioned by designer one in his interview. Shortly before answering one of the questions with that example, he had indicated that the Coast Guard tends to share log-ins to those type of systems so that others may view its output. This may be effective to a certain extent in communicating with select Port partners, but has issues with much of the desired information being hidden away behind password protected firewalls.

Something for everyone

APAN was developed to act as an unsecure communication bridge amongst all port partners in a sort of community of communities, but due to the systems openness, is not suitable for passing threats that would be associated with terrorist activities, it would only be suitable for natural disasters. ALMIS was previously adapted in the aviation field of the Coast Guard as an inventory management tool that allowed planners to view what asset status was. When planners within the Coast Guard witnessed the utility of the program, it was further adapted to the marine environment. The system is very beneficial to the Coast Guard, but requires CAC access for it to be used, which limits any users outside of the Coast Guard from using it without a lot of administrative paper work, to get non Coast Guardsman cleared into the system.

Nothing for everyone

These systems were developed to meet a particular organizational need with little thought given to interconnectivity between collaborating agencies. This may be a manifestation of the turf wars, which were mentioned by two of the five interviewers. Far more plausible, is that these systems, which are in common usage today began their paths to mature systems well before the events of 9/11 when it was not that important of a design consideration within the Coast Guard. As was indicated by the Technical Director, systems went through one design pipeline or another and from inception to realization of the capability is usually in the range of 10 years. An inconvenient fact of this, is that the service lives of these systems will be greatly reduced in the heightened threat environment that is forcing more interconnected systems. However, it does provide the ideal place to begin new system requirements.

B. How would one of the existing multi service information sharing tools be improved to selectively incorporate information useful to any roles that are involved in harbor operations?

This question was created while the initial literature review was taking place. During this time, there appeared to be an abundance of systems aimed at the sharing of information but depending on who was interviewed, the opinions of their functionality varied greatly. Thus, from a systems engineering standpoint it would be both more economical and timelier to enhance the features of an existing system or perhaps roll desirable features of one system into another creating a hybrid which would meet all design requirements.

ALMIS

When the Operator was offered an example of a new systems capability he had indicated that "*ALMIS does a lot of that but it really does not follow the operator beyond the docks.*" To adapt ALMIS to meet all system requirements of an information sharing system, would be to accelerate the TWIC program and get security clearances for all individuals who work in or around harbors. There is guidance to do just that but it is not without its controversies as MIST researchers had discovered. The addition of an authentication type would present few problems but the setting of Access Control Lists (ACLs) on each one of the data sources the system pulls from could prove difficult for the system to resource.

APAN

From an office discussion with a subject matter specialist regarding candidate systems which could possibly be considered, it was indicated that with APAN there was little that could be done to secure different channels and limit access to a user group that either had a Common Access Card (CAC) or one of the TWIC cards. These Broad design changes required to get this system to conform, would make it a completely new system.

Homeport

Homeport, when discussed with designer one, highlighted one of its strong features as, "*The Coast Guard uses many channels to get information out…*" and indicated that Homeport was quite good, but it was an access issue that precluded it as a possible solution. Mostly due to its core functionality lying behind Coast Guard firewalls, it would be difficult to adapt it to the design requirements of a future solution. The portal approach is worth consideration but there needs to be a higher degree of user interaction associated with the system that would allow spot users to post real time information quickly to either selected users or broadcast. This was another insight garnered from both the Subject Matter Specialist and the Operator.

C. What are the human factors that are alleviated by FACE-TO-FACE meetings which may be addressed by the introduction of a technology?

This question was designed to assess the value that the face to face meetings were bringing back to the communication system that had been lost in the technological chaff. It was felt while drafting it, that it would get at the true expectation of what makes an ideal information system important to its target users. Also, to pull out the shortcomings of going directly into technology implementation before doing proper assessments of target user groups. The Operator spoke to the shortcomings of the meetings with his statement: *"It is a great snapshot of the fragmentation of information sources."*

This question was looked at quite closely in the Boston workshop as illustrated here

> First, there was strong recognition among the workshop participants of the purpose and value of collaboration for ensuring port security and related commercial viability in the Port of Boston. This acknowledged "strategic necessity" is the foundation for successful collaboration and has been recognized as key in other MIST events. (Salem, 2011)

Familiarity with port partners

Prior to the events of 9/11 many of the different offices that form today's port partners could not tell you the name of the person that worked just across the street from them. When thinking was elevated by the events of 9/11, a long look was taken at methods of conveying threats via technological means and was heavily scrutinized as being one of the chief causes of the communication breakdown. Boston took a pragmatic first step and went back to face-to-face meetings where it was discovered just how diluted they had become to security issues. Few other ports have gone to this extreme, but certainly, the higher threat areas took similar actions. As it turns out, other benefits started to manifest themselves in the form of participants building text lists so that they were able to send off quick notifications when relevant information changed. This is similar to what the Valued Information at the Right Time (VIRT) method promotes today. All that this discovery required, was getting people to sit down once a week in the (Port Operator's Group) and discuss concerns. One interesting opinion came from the operator, in that he felt the meetings were an absolute necessity when faced with all of the mandates being forced down upon his operation.

Interconnection

The already mentioned text networks that formed almost instantly, were really just the beginning of beneficial realizations, as personnel relationships spawned, and knowledge of what was important to each other's agencies became known to all. This led to efficiencies of communications in the hypothetical form of Boatswain Mate First Class (BM1) Smith with the Coast Guard knowing that the CBP agent Fernandez mentioned a Be On the LookOut (BOLO) at last week's port operators group meeting. BM1 Smith texts Agent Fernandez directly when he comes across a suspect of similar build, dress, ethnicity, and so forth. Efficiencies like these, remind researchers and port partners why they should be interested in participating in discussions of new systems that will provide similar results.

Recognition of problems before they happen

There can be no value ascribed to the urgency of a threat when it is conveyed, face to face by a person who knows the ramifications if that threat is realized. Often what breaks a chain of horrible events, is a person who is outside of its normal discussion pointing out an angle that through experience has become transparent to those discussing it. Often the more individuals looking at a problem, subtle risks will be revealed that highlight a need for contingency planning. In information assurance this concept has led to the development of highly effective Host based Intrusion Detection Systems which the author believes to be a good analog the problems associated with building more effective communications systems.

D. How can an information sharing structure be designed that leverages Boston Harbor's findings and be scaled for use by other harbors?

There is a broadly accepted belief that terrorists will not strike a well-protected harbor like Boston, when there are any number of smaller ports up and down our shores which represent far easier entry. Thus, any solution that is considered needs to work at the smaller harbors as well as the larger ones because they both comprise the threat surface. The Coast Guard and CBP with their small numbers cannot possibly be expected to secure every inch of these harbors without the introduction of an information sharing system as a force multiplier that would also canvas the smaller ports.

Single point mooring concept in which all stakeholders truly have a stake

As the operator had pointed out repeatedly in his interview, *the single point mooring* for regulations would take the United States a long way toward building a system of information sharing that all would benefit from. In its current state, where regulations are put out, for actions that have been carried out for years and are delineated in several other places, the system is broken. Thus, it is known what is broken. To fix it, all must come together and give of their time, monies, and efforts. Once this regulatory side is fixed, and agreed to by all, the other portions will work their way through similar channels and meet the same success.

Agreements between all port partners as to what needs to be shared

Clear functional boundaries have to be agreed on, as well as what is required to be shared and with whom. Classification of information has traditionally been a stop for actions in communication chains as was indicated by three of the five interviewees over two different interview questions. What presented itself to MIST researchers was a sort of *last mile* problem of getting all harbor personnel through the proper screening to gain access to information streams. Indeed, one of the largest port partners in Boston, MASSPORT continues to use their own ID cards and will do so for the near future. That is, until all stakeholders can reach an accord on most issues. This may prove to be an excellent area to prove that connections can be made and when they are made tremendous efficiencies may be realized. It was pointed out in MISTS Boston report as a next step for Boston to Have Massport connect with the Coast Guard. If this connection could be made, many of the other port partners would jump on board and progress would ensue.

Start designs from position of information glut

Designer two, aside from being perfectly candid in all of her responses, also imparted the wisdom of *starting designs from the information glut posture*. Meaning, the Coast Guard and many other organizations are continually in a state of information overload. Which is to say, that they have so much information that they are inundated with it, and valuable information gets lost in the chaff. By most outward appearances a smart push system from some form of Dublin core is required to not burry operators.

All of the thesis questions have been covered by laying them out, then addressing the themes that had emerged over the course of thesis research. The themes themselves could be considered to outline the lessons learned by both the Coast Guard and other agencies, which hold a great deal of value to future systems requirements discussions. These themes and research questions shall form the basis of the discussion and framework of Chapter V conclusions, as well as recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATION FOR FUTURE WORK

A. DEEPER LEVELS OF FRAGMENTATION

What has emerged as an overall finding from the both the MIST seminars and interviews that were conducted for this research, are the deeper fragmentation of communication of threats and the sidestepping of regulations to accommodate one partner's needs, which ultimately drive system development. When these systems are developed without requisite input from harbor operators, their utility is diminished and can therefore fall short of overall regulatory synergies. Yet at times, best practices have also emerged as a result, such as face–to-face meetings conducted in Boston. Yet, these may soon become antiquated through technology and the demands of the people whom attend them as a result of time demands from their own jobs.

1. There is not a "one size fits all" solution to all port partners communications needs and it is likely that one has not been conceived as of the writing of this thesis

Although there are many examples of useful communication solutions, which can convey threats, few of these would match up with even 10% of an overall system requirements, which might achieve the coveted one-size-fits-all label. The more pivotal underlying issue is influencing all port partners to agree to a singular standard for anything that they would agree to and thus share knowledge to oppose discovered threats. This point also highlights one of this thesis's most important points, that whatever the communications solution turns out to be, to have all partners concur, it must be grounded in the trust that the Coast Guard has earned in terms of communication sharing.

To try to improve any one of the existing communication systems to meet all partner's needs would be difficult at best. A much more plausible solution may be to develop a new system that has concurrence from all partners from conception to final use. One of the best practices mentioned by MIST was the USCG alert system that may be included in a future system. This already proven system would likely require very little resources to convey information whether it be terrorist threats or environmental issues as operators already employ and trust this system. This system has also earned a reputation for accuracy and parsimony in that it was not used very often, and only when there was actionable information that needed to be retrieved or conveyed.

2. A lack of familiarity with the recipients of information that causes partners to withhold and not share

MIST’s careful analysis of partner motivations revealed some of the problems that may be addressed to bring partners to continue development. Motivations that in particular, can be surrogate communications systems for the development of capabilities in communications systems. For instance, the desire to avoid litigation by airlines and the desire of commercial shipping companies to avoid costs provide constraints of systems that are transparent to users in some instances yet completely visible in others. In a *smart push* type system, the surrogate user needs to find the filtration needed to garner partner trust and a willingness to share threat information.

The results of this research also reveal that the findings from Boston Harbor can be scaled to any size harbor. This is because Boston Harbor crosses so many of the functional areas found in all harbors. There are few harbors that possess functionalities and issues not found in Boston. For example, the presence of an airport in close proximity to Boston Harbor allowing airlines partners who move cargo to sea going commercial shippers is a characteristic common to large harbors, yet could easily be removed from the concerns of smaller harbors. Thus, the shared understanding of the issues that occur at Boston may provide quick and easily related issues to a smaller port.

A Technical Director spoke to another when he indicated that sharing the information in a trustworthy method. His concern centered upon who he could trust to protect that information and convey it in a manner that is acceptable to its originator. The Technical Director also indicated that if a technological solution is to be reached, it would have to be one that employs strong encryption that would potentially stay with the data from cradle to grave and would ensure that only intended receivers get these messages. With recent communication systems being very publicly defeated, e.g., wiki-leaks, many people are less trusting of technology for their lives or their security.

Finally, what can hamper the building of a trusting relationship to transfer information correctly can also arise from failed or unresolved historical issues from the either the companies or individuals of those companies. Similar to the ways that in small organizations word of a disaster travels fast, as do the mistakes of today's companies who sometimes fail to safeguard their highly personnel identifiable information. Usually all that it takes is one unfortunate event and the next day the company can be out of business due to their tarnished reputation. Companies and their introduction of new technologies should consider these issues as development occurs.

B. FUTURE WORK

1. Exploration into determining how to ensure all partners commit resources to a common system development

Lately, this has been one of the chief focuses of MIST and will continue to perplex those who attempt to resolve given that large number of stakeholders. As noted earlier, to improve or build a better communications infrastructure, MIST's work here will continue to be instrumental to unanimously design successful information sharing systems. Understanding the motivations during the requirements phase may better illustrate areas to focus on as well as areas to avoid. A proper study of developing both a tailored understanding of individual harbor issues as well as maintaining institutional trust between port partners using adequate security may be beneficial.

2. The determination that a single information sharing system needs to be designed and implemented for a partners to communicate

One organization has to take on the monumental task of getting organizations to agree and more importantly to feed a discussion of requirements of a singular new system. As previously discussed the systems that were developed to meet individual partner needs has only driven organizations away from one another and strengthened barriers against efficient communications amongst all. If multiple organizations' issues could be focused and agreed to by all, that may form the basis of an overall design solution and possibly lead to an approved and universally implemented system. Ramifications of this may ripple through other organizations suffering similar circumstances like the Joint Services Command's efforts to create one radio that can be used by all organizations.

3. Developing a map of how a communication system will have to develop to please all partners

To develop an overall design, organizations, it seems, will need to agree that even though their individual information sharing system, which they developed for their own purposes, works for them, it can be greatly improved in value if it is extended to all partners and thus flawed when compared to a universally accepted information sharing system.

To generate this map, trust will have to be the cornerstone for every decision as previously illustrated by the Coast Guard. DISA has begun working on this issue, yet has remained somewhat secretive about its solutions. As can be imagined, once released, adversaries will work to develop methods to subvert security of that system.

4. Organizations sharing information may also mean sharing sources, and perhaps loss of identity

To coax partners to admit where they have made mistakes, or run into difficulties in their own systems will be difficult, yet may also be the most beneficial to the overall systems development. There are many stakeholders who believe that this is probably the chief issue driving "turf wars," which is to say that organizations are often embarrassed of either the data that they have collected or the manner in which they have collected it. For those organizations in this fiscally charged environment, there is a fear of losing control of their own systems and subsequently losing potentially their organization's identity. This is a difficult organizational problem, yet needs to be explored and perhaps resolved so that we might ultimately secure our harbors with the best information sharing system conceivable.

APPENDIX A

A. MINDMAPS OF INTERVIEW QUESTIONS

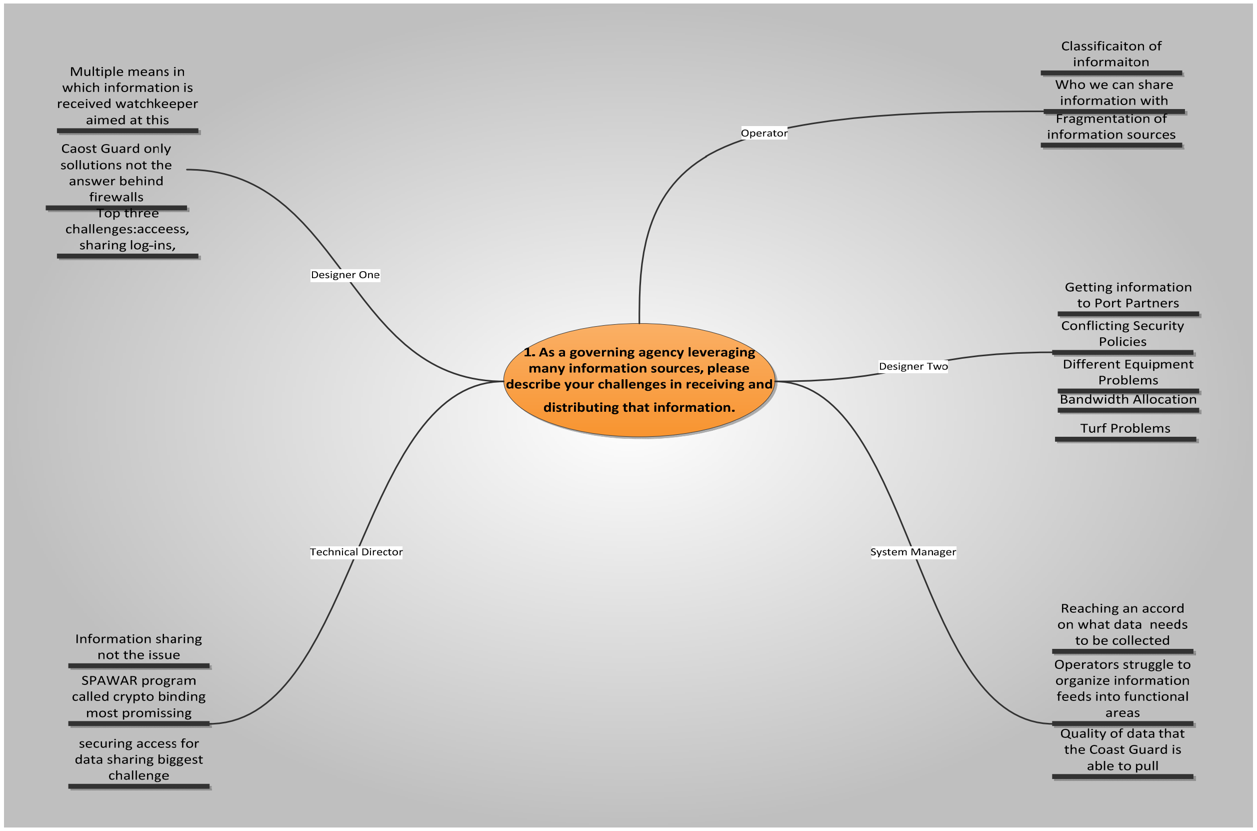

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.
Designer One
Multiple means in which information is received watchkeeper aimed at this
Caost Guard only sollutions not the answer behind firewalls
Top three challenges:acceess, sharing log-ins,
Operator
Classificaiton of informaiton
Who we can share information with
Fragmentation of information sources
Designer Two
Getting information to Port Partners
Conflicting Security Policies
Different Equipment Problems
Bandwidth Allocation
Turf Problems
Technical Director
Information sharing not the issue
SPAWAR program called crypto binding most promissing
securing access for data sharing biggest challenge
System Manager
Reaching an accord on what data needs to be collected
Operators struggle to organize information feeds into functional areas
Quality of data that the Coast Guard is able to pull

Figure 3. Interview Question 1

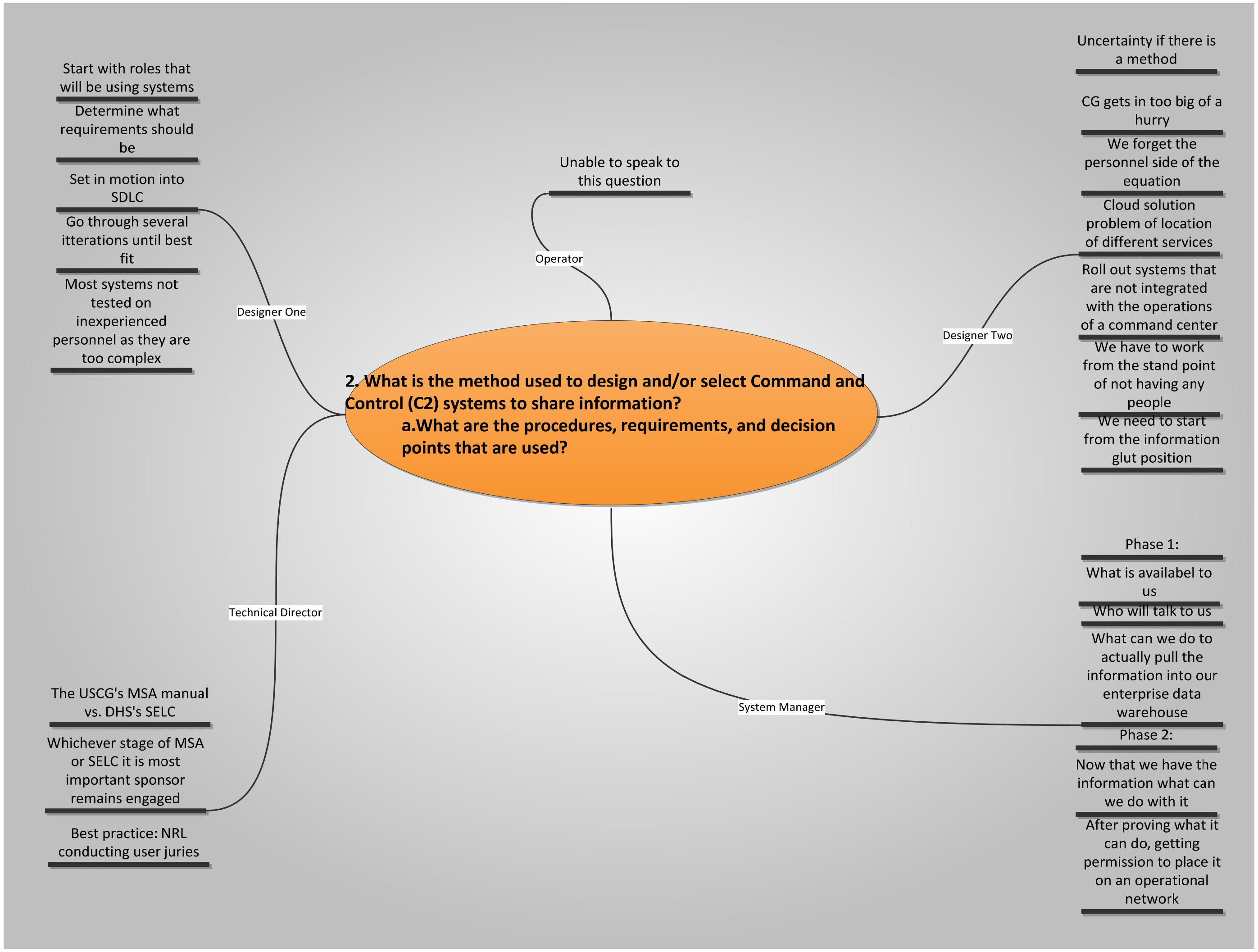
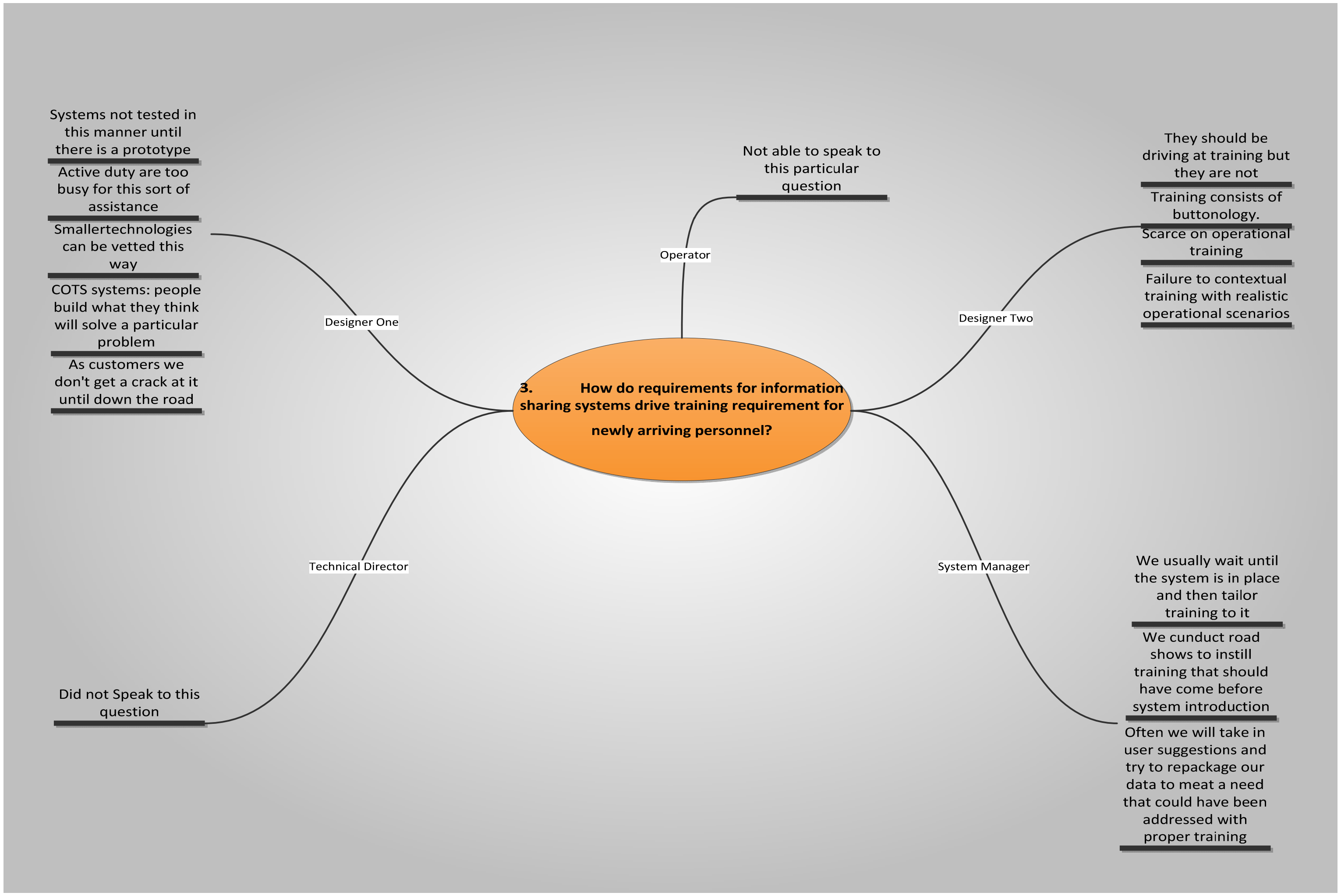

2. What is the method used to design and/or select Command and Control (C2) systems to share information?
a.What are the procedures, requirements, and decision points that are used?
Operator
Unable to speak to this question
Designer One
Start with roles that will be using systems
Determine what requirements should be
Set in motion into SDLC
Go through several itterations until best fit
Most systems not tested on inexperienced personnel as they are too complex
Designer Two
Uncertainty if there is a method
CG gets in too big of a hurry
We forget the personnel side of the equation
Cloud solution problem of location of different services
Roll out systems that are not integrated with the operations of a command center
We have to work from the stand point of not having any people
We need to start from the information glut position
Technical Director
The USCG's MSA manual vs. DHS's SELC
Whichever stage of MSA or SELC it is most important sponsor remains engaged
Best practice: NRL conducting user juries
System Manager
Phase 1:
What is availabel to us
Who will talk to us
What can we do to actually pull the information into our enterprise data warehouse
Phase 2:
Now that we have the information what can we do with it
After proving what it can do, getting permission to place it on an operational network

Figure 4. Interview Question 2



3. How do requirements for information sharing systems drive training requirement for newly arriving personnel?

Operator

Not able to speak to this particular question

Designer One

Systems not tested in this manner until there is a prototype

Active duty are too busy for this sort of assistance

Smallertechnologies can be vetted this way

COTS systems: people build what they think will solve a particular problem

As customers we don't get a crack at it until down the road

Designer Two

They should be driving at training but they are not

Training consists of buttonology.

Scarce on operational training

Failure to contextual training with realistic operational scenarios

Technical Director

Did not Speak to this question

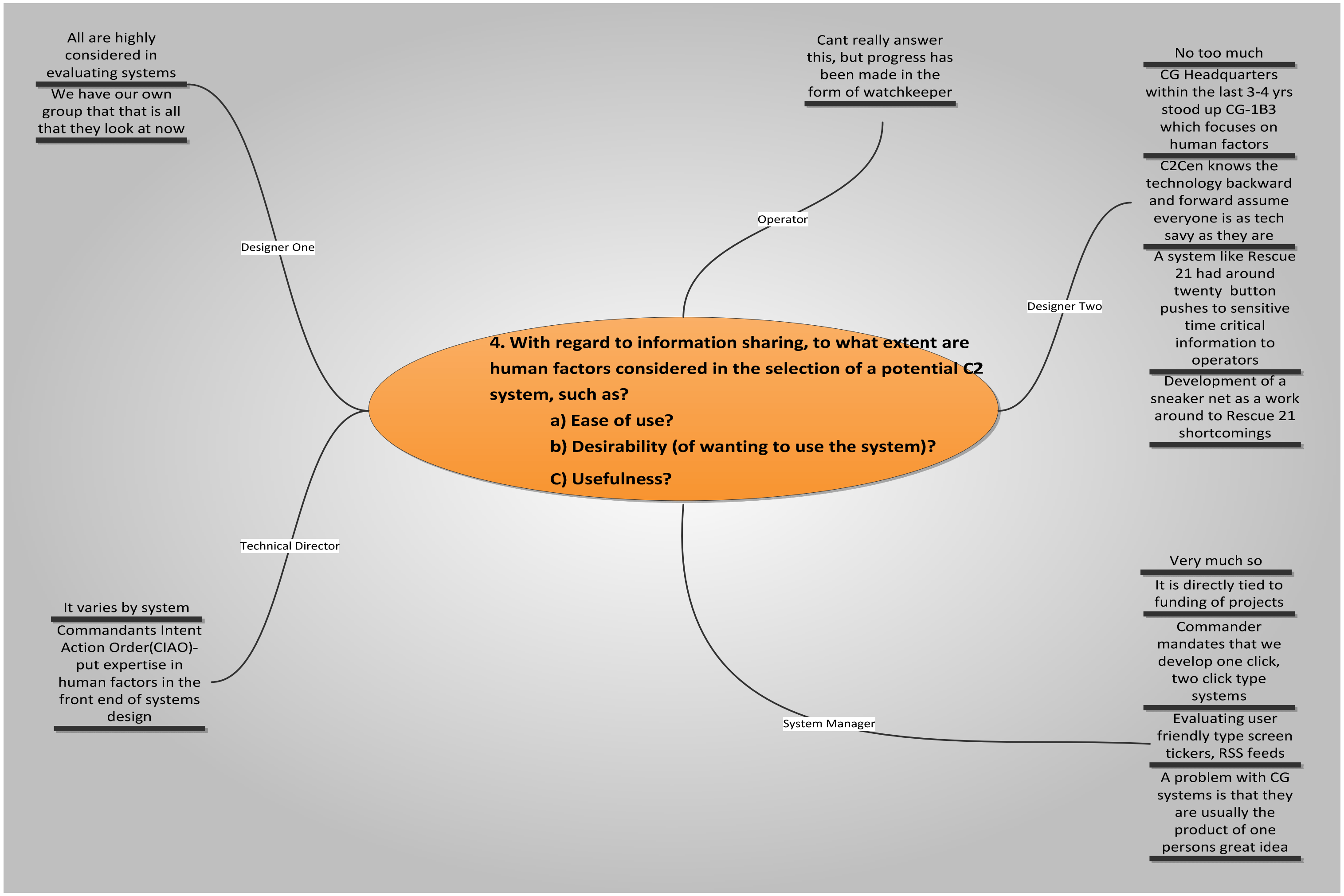
System Manager

We usually wait until the system is in place and then tailor training to it

We cunduct road shows to instill training that should have come before system introduction

Often we will take in user suggestions and try to repackage our data to meat a need that could have been addressed with proper training

Figure 5. Interview Question 3



4. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?

a) Ease of use?

b) Desirability (of wanting to use the system)?

C) Usefulness?

Designer One:

All are highly considered in evaluating systems

We have our own group that that is all that they look at now

Operator:

Cant really answer this, but progress has been made in the form of watchkeeper

Designer Two:

No too much

CG Headquarters within the last 3-4 yrs stood up CG-1B3 which focuses on human factors

C2Cen knows the technology backward and forward assume everyone is as tech savy as they are

A system like Rescue 21 had around twenty button pushes to sensitive time critical information to operators

Development of a sneaker net as a work around to Rescue 21 shortcomings

Technical Director:

It varies by system

Commandants Intent Action Order(CIAO)- put expertise in human factors in the front end of systems design

System Manager:

Very much so

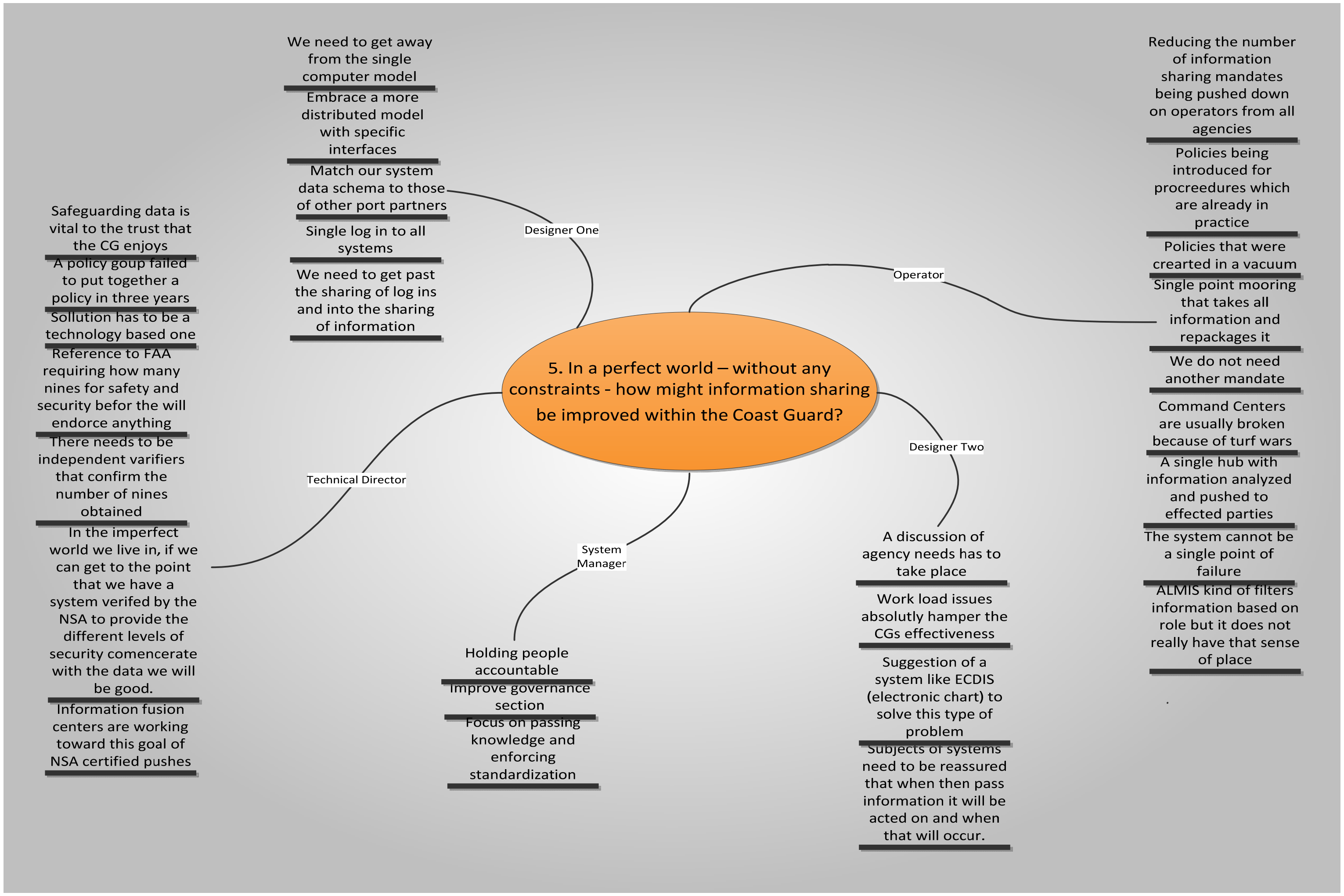
It is directly tied to funding of projects

Commander mandates that we develop one click, two click type systems

Evaluating user friendly type screen tickers, RSS feeds

A problem with CG systems is that they are usually the product of one persons great idea

Figure 6. Interview Question 4



5. In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?

Designer One

We need to get away from the single computer model

Embrace a more distributed model with specific interfaces

Match our system data schema to those of other port partners

Single log in to all systems

We need to get past the sharing of log ins and into the sharing of information

Operator

Reducing the number of information sharing mandates being pushed down on operators from all agencies

Policies being introduced for procreedures which are already in practice

Policies that were crearted in a vacuum

Single point mooring that takes all information and repackages it

We do not need another mandate

Command Centers are usually broken because of turf wars

A single hub with information analyzed and pushed to effected parties

The system cannot be a single point of failure

ALMIS kind of filters information based on role but it does not really have that sense of place

Designer Two

A discussion of agency needs has to take place

Work load issues absolutly hamper the CGs effectiveness

Suggestion of a system like ECDIS (electronic chart) to solve this type of problem

Subjects of systems need to be reassured that when then pass information it will be acted on and when that will occur.

System Manager

Holding people accountable

Improve governance section

Focus on passing knowledge and enforcing standardization

Technical Director

Safeguarding data is vital to the trust that the CG enjoys

A policy goup failed to put together a policy in three years

Sollution has to be a technology based one

Reference to FAA requiring how many nines for safety and security befor the will endorce anything

There needs to be independent varifiers that confirm the number of nines obtained

In the imperfect world we live in, if we can get to the point that we have a system verifed by the NSA to provide the different levels of security comencerate with the data we will be good.

Information fusion centers are working toward this goal of NSA certified pushes

Figure 7. Interview Question 5

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

A. INTERVIEW TRANSCRIPTIONS

1. Operator Interview

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.

Well right off the bat classification of data and who we can distribute it to. What players can get what information in a timely manner?

That also holds true for us receiving it from other sources like JWICS

Interconnectivity: no common system of other core partners for sensors.
Watchkeeper is attempting to do this now

CBP works for unclassified material but it is not fully plugged in.

Having the linkages already in place so that our core partners already have an idea of what type of information we require and vice versa, typically dependent on all watch standers to be sharp enough to know that the information that they are handling may be relevant to the Coast Guard.

The JTTF which is FBI oriented and the BRIC (Fusion Center) lots of gang related information in there. It is a great snapshot of the fragmentation of information sources.

> POG (Port Operators' Group … in Boston, the POG is what other ports may call the Harbor Safety Committee. The HSC is a small subset of the POG, which includes expanded port-oriented partners.)

Fusion Centers

Harbor Masters

Lots of redundancies in the information at many of these meetings

- *Specifically, what challenges are encountered in information sharing between the public and private sector?*
- *What are your top three challenges?*

2. *What is the method used to design and/or select Command and Control (C2) systems to share information?*

- *What are the procedures, requirements, and decision points that are used?*
- *How do requirements for information sharing systems drive training requirement for newly arriving personnel?*

  This is a question for the Techies.

3. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?

I can't answer this as we are not designing, there is thought going into it, as evidenced by Watchkeeper, that it is a good example of us tailoring a website aggregator that is configurable that we are beta testing. Works mostly in the displaying of information which indicates an awareness of making these more user friendly. We have come a long way but to what degree he can't say.

- *Ease of use?*
- *Desirability (of wanting to use the system)?*
- *Usefulness?*

4. In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?

My pet issue that I am trying to shore up; you are aware of the incredible number of information sharing mandates that are being pushed down on us which are really already being done in practice but there really is no efficiency in the manner in which it is categorized.

MOC/REMOC signed by COMDT and ICE coordinating local efforts that is a carbon copy of every other edict that is out there. My problem is how these are so fragmented and seem to have been created in a vacuum. If you take a closer look at the MDA that is supposed to be acting as a hub that has tentacles into all the agencies could be implemented into the Maritime information sharing environment. Single point mooring that takes all the information in and aggregates it (repackages it) we don't need another mandate. Command Center models don't work because of turf wars, what everyone is working toward is one of the virtual collaborative systems. MISLE and MAGNET, Watchkeeper that allow the users to configure the information that is relevant to them is tailored to them. Everyone coming up with their own solutions is not working.

A central hub analyzed and pushed to the correct parties that are a single system that is not a single point of failure. Refer back to the MDA model which focus on a hub model that presents the information that can be pushed automatically.

[An example proposed by the interviewer could be an ideal system, role based; the technology needs to have a sense of place. Small boat coxswain with a PDA changing roles from that of the OOD to that of Coxswain and the information that he needs is tailored to that role.]

ALMIS does a lot of that but it really does not follow the operator beyond the docks.

2. Designer One Interview

1. *As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.*

    Specifically, what challenges are encountered in information sharing between the public and private sector?

We have probably our biggest challenge is our means of having all the users have similar means to receive the information. The Coast Guard uses many channels to get information out. Some examples of these may be Homeport which is on the web, traditional ones via radio broadcasts. It has been a challenge; this problem has been realized for a long time, going back to Marine Transportation Systems Reports back in the late 90s. The National Academy of Sciences/ Marine Transportation Systems Reports are the Coast Guard sometime around 2000. Watchkeeper is a new tool which is under development in the Coast Guard Acquisitions, and I have had some involvement with that, not currently, but I do know that it was prototyped in Charleston South Carolina and it was created to be an interagency operations center piece. So, it would have the ability for our port partners to engage for security type information where they could simply login. As opposed to the Coast Guard only systems that existed behind the Coast Guard's firewalls, it was the constraint that it has its own security that meant you had to log in from outside of the Coast Guard's data network allowing outside users to log in as well. I believe the system lives outside the Coast Guard's Data Network and is in our DMZ for the kind of non-militarized systems. C3Cen developers could answer a lot more questions on that. I am not sure where that is at in the Coast Guards acquisitions cycle but that is a system which has been very short of resources lately.

What are your top three challenges?

Well I am a researcher so I don't really face these challenges directly but we do help develop solutions for them. The whole issue of access, like with watchkeeper and providing accounts that grant access to watchkeeper from within other systems. I think that is still going to be a big hurtle because those other organizations like DHS, Local Law Enforcement, and Port Partners all have their own systems and we don't seem to be able to make progress in getting our systems to talk to one another which is where I feel the biggest challenge is. We don't share information as much as we share log-ins. Watchkeeper is being developed in service oriented architecture, so what it is doing is accessing the existing databases which also connected to our inside service architecture, we have an enterprise service bus, though there are services that provide the data from various sources be it SANS vessel arrivals or AIS for vessel positions, whatever. All those services provide information to the enterprise service but to watchkeeper as a consumer of those services. Then you have services within watchkeeper that allow users to do queries and find out information about things. So, Watchkeeper is being built the right way in that it is not duplicating databases or doing any of that. In terms of being a wrapper for separate technologies it is and it should be. [Interview inquired about freeform queries] Watchkeeper does not really do freeform queries but there are predesigned queries. However, watchkeeper I think is using both Posting and polling for its data.

2. *What is the method used to design and/or select Command and Control (C2) systems to share information?*

Watchkeeper again which is in the Coast Guards Acquisition Life cycle in that you have defined roles such as sponsors, and sponsors representative, whereas most of the systems in common usage today are in the SDLC system for maintenance. So they have configuration boards they have all the areas it was fairly structured with SDLC. In R&D we get more of the: we think this is an interesting system and we want you to go evaluate it.

What are the procedures, requirements, and decision points that are used?

We often help develop requirement but we do not produce them, those come from the program. We do research that helps them figure out what the requirements should be, and that is the operational requirements document not the award but that is just one piece that is the foundation document to determine if any of these get accepted. That is just one piece but I would argue it is one of the most important ones. We have a process that is supposed to be followed, but quite often things get started and there is a candidate technology out there and the award is often back fit to express the need for the technology. Now I'm not saying that is not necessarily bad; as when you are working on requirements you have to be cognizant of what potential solutions are out there. You cannot just develop requirements in a vacuum or you will either: one, specify things that can't be done or two, you will be specifying things that are very easy to do. You have to go through several iterations to get the best solution. That being said, we do have our acquisitions decision points one, two, and three that are mixed in from concept development to full production.

How do requirements for information sharing systems drive training requirement for newly arriving personnel?

Generally not tested in this manner because to put one of these systems into a unit is kind of a big deal and we generally don't bring real operators to look at systems set up wherever. These types of systems have so many connections that they are hard to prototype. There are so many pieces and parts that have to have inputs and outputs to them it is just not practical. Generally, it is done in a more formal fashion where you have an actual prototype site determined and there is training involved but these people that are testing have their regular jobs that they are dealing with as well and it is no small thing to get them to look at something for you. Smaller technologies that we are interested in installing on boats, we can do that with local units, but again there is a formal process there. [The interviewer postulated that many of the technologies that are being tested would have had a fair amount of user feedback if they are COTS type systems]

Well, I'm not sure. Like a lot of software that has been built by designers the people designing it build what they think is right, hopefully they have some operational experience where they can scrutinize their own process to make sure it is a good interface. As customers, we don't really get a crack at it until it is pretty far down the road.

3. *With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?*
    - *Ease of use?*
    - *Desirability (of wanting to use the system)?*
      Usefulness?

These are all highly considered in evaluating systems. We often look at those factors in whatever system we are considering. We have a group that does human factors at the R&D center and they often get called in to look at systems to evaluate them for those concerns. Therefore, it is prominent that we put it right up front for the evaluation of any system.

4. *In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?*

Everybody still has this single computer mentality that everyone logs into one system to get there information where I think that we need to develop more of the distributed model and have specific interfaces defined for system to talk to each other. So that users in different communities whether it be within the Coast Guard or our partners can maintain their own system and connect to our system so that we can share whatever information we have determined needs to be shared back and forth with them in a more streamlined fashion. An example maybe, a watch stander that does not have to have logins to four different systems to do their jobs; instead they have one system that has everything that they need fully integrated together. We have been working on a project to achieve that sort of thing with DISA in a net centric enterprise services information sharing system that the Coast Guard could share with our partners in the DoD. (Interviewer mentioned the DISA cloud services that are being developed for the Coast Guard) I have no idea where that is, I got out of that part when they started it. I don't know if the cloud is just the same stuff we were calling the net centric enterprise services that tended to be not network centric repository but a controlled infrastructure for sharing information. I am not sure if they are using the GIG to do much of that or not. I was only familiar with that through the information that we had in common with DoD like vessel tracks in AIS and we were also working on vessel arrival data to share that data and whoever could subscribe to it through the DISA services. So somebody would subscribe and they would just get packets of XML data and that was what we were sharing. They could just take that data and put it into their system and use it anyway that they wanted to and we did not have to worry about the semantics of nomenclature of the systems that they were working on. [Interviewer asked what semantics they were interested in of ours for their own pragmatic goals] Usually they were wanting log-ins to our systems which we don't give out to just anybody and it highlighted the difficulty in getting someone access to systems. Five years from when we started looking at this information sharing we are still sharing log-ins and not information.

3. Designer Two Interview

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.

- *Specifically, what challenges are encountered in information sharing between the public and private sector?*

I can't talk from my own experience, but I can talk about the work that I had done with sector command centers where we have a number of difficulties sharing information with our partners. Like Customs which its part of DHS and has their own firewalls and computer systems; we also have state a local law enforcement agencies. We may work together with these partners on a number of different things for example when I worked down in Sector Miami which has number of law enforcement missions that they prosecute daily in which it is possible that they will be working with Florida Fish and Wildlife Services out there, or perhaps Customs. The problem that is most frequently observed is different port partners have different levels of classified or unclassified information that we can share with them. For example we might be able to provide Customs with Secret info; but we might only be able to provide local law enforcement with UNCLAS, because they don't hold a security classification. So, one set of information can't be seen by everybody. Also, because Customs has their own set of rules of what they can and cannot share, and if our firewalls don't meet the requirements that their firewalls do, we cannot share -- which translates to both policy and equipment type problems that get in the way of sharing the information we would like to share. I think that we also have some equipment problems in bandwidth allocation where someone may be transferring blueprints for a cruise ship that everyone is interested in doing a joint boarding on. We might not be able to send the blueprints because our network bandwidth isn't able to accommodate such a large file in addition to all the other things that are already on our network. Video data often has to be sacrificed for this reason. There are a number of problems that make it hard to share from a tactical standpoint as well. One problem in particular that keeps coming up is radio messaging between these different agencies. Whereas the Coast Guard deals with channel 16 for the uncovered stuff, i.e., radio communications "in the clear," the local police use a completely different set of bands when they are transmitting messages. Therefore, we do not have the same equipment that transmits over the same radio bands which are crucial to be able to talk to one another. In the past we have done some projects helping specific locations do interagency communications and it is quite a hard job because you end up needing a different set of equipment and people do not want to be saddled carrying two or three different kinds of radios so that when they have to talk to customs they have got this radio, and when they are talking to Miami Police Department they have got a different radio. It can be difficult. There is also the question of what kinds of information do my agency need to keep just for itself for what we do? Versus, what am I willing to share with my other partners? Therefore, there is a whole bunch of little problems there. One could most aptly characterize these problems into two broad categories: technology and turf battles, i.e., the mentality that I am special and you don't need to have your nose in my business.

- *What are your top three challenges?*

I don't think that I can rank those; it would have to come more from the operational folks. [Speculation] It is so easy to point a figure at technology and say ok well it does not work so how can you… but even when they were doing the interagency communications thing a few years back, [although I was not a part of it, a friend of mine was heading it up] and even when they were able to provide the technology, that was when you would see the policy and turf issues start coming up. It is hard to include everyone because the people from different agencies have different training, different backgrounds, there is organizational culture that differs between these groups. Now, suddenly they are all trying to play on the same field. One of the things that they found out in that project was some of the agencies (not sure which ones) spoke in codes so an example of a black speed boat coming from this direction, there would be a code seven or something like that. So, it gets right down to what exactly you say when you are trying to communicate with people that do not have any knowledge of your vocabulary, and cannot understand what it is that you want; therefore, they cannot do what is needed because of their lack of understanding.

3. *What is the method used to design and/or select Command and Control (C2) systems to share information?*

There is a different method -- if there is a method at all -- depending on who is designing and developing the system. Which is part of the charm of the Coast Guard … in that we have a number of different groups that do this sort of work and it is something that we really need to do a better job of? Speaking around this to maybe give us a little context, I think part of the problem is that we get into too much of a hurry. Somebody says we have got this problem and we have money, congress just gave us something to do; let’s throw money at it, let’s fix it, and let’s get onto something else. In our haste to do something, we do either whatever seems easiest or “this technology looks really cool” and go with that. Thus we get too technology focused and we forget about the people and the tasks that need to be supported by that technology. Now, I am on my human factors soapbox. [Interviewer mentioned own misunderstanding that the DISA cloud would be the solution to 90% of our information sharing problems] When the cloud does come into service, the location of different services will be totally obscured from the user. The Coast Guard had a Hawkeye system that we put together for one of our first ventures into security and surveillance of ports and waterways. Hawkeye was part of the work that we were doing in Miami so I will pick on them. Hampton Roads was also a site, so I will pick on them as well. Prior to this venture, we had nothing that would allow watch standers to see vessel traffic in and around the port, so anything was considered to be better than what we had right then. C2CEN put together a very nice prototype that made for an excellent research tool in which we could put video cameras out there, we could get AIS tracks coming in, and we got radar tracks that would provide input into geographical information system. Therefore, now you can see who is out in your port, you may not know who they all are, but you at least know where vessel traffic is coming from, you know where it is headed. Hawkeye, as a prototype was a really great tool to help you understand what the Command Center watch stander's need is for vessel traffic info and what the capability needs to be to fill the need for vessel traffic info. The mistake that we made was "well gee that looks pretty good, let's give it to everybody." We started rolling out something that was not thought through very well, isn't integrated with anything else in the command center, and just becomes one more tool that you have to have a body sitting in front of. Thus the system, which could have provided very useful data, could not because it was not integrated with any other systems and was relegated to being nowhere near as useful as it could be. This is the way that we should not develop new equipment. I am sure that every command center that has that system is really happy because they can see things that they never could have before; but it requires an extra watch person to man a terminal, and the Coast Guard never has extra people. If we had just thought a little bit more about how to implement a system such as this and really nailed down the integration part (who should be doing this, who should be getting these data feeds…) A pretty good example of "stick it out there, find out that it is wrong…), but you do learn something from it. The problem comes in the form of you just have to deal with it for the next ten years until we get funding to do something better. I see that as our biggest problem; that we don't look before we leap. It makes sense at a very high level, absolutely, that we need that capability, but we need to understand who needs it, what information is necessary, how does it fit into the rest of the jobs that we are asking these people to do for us. All those human factors and procedural type of things need to be addressed.

[Interviewer mentioned an infrastructure issue of using a lot of servers to handle this great glut of information] Especially in a busy port like Miami where you have 40+ vessels a day coming in to drop or pick up cargo, cruise ships, and an abundance of recreational boaters out there doing who knows what. There is a lot of data to look at and what has not been done yet, what there has not been any R&D on, is the number of people per unit of data that this type of system demands. The sheer volume of information coming into a port like Miami would not be practical for a single watch stander to leaf through and draw any actionable intelligence from. There has been some on and off R&D efforts to develop some kind of a decision support tool that will look at different vessel tracks and do the comparison of logical operations to look for anomalies; e.g., is this vessel going where a vessel of this type “should” be going to sound an alarm. Another thing that happens when a system like Hawkeye gets put into a command center is that we have never developed any type of training for watch standers to be able to determine what is normal, and what we should do with this now that you have it on your desk. So we just do things, and granted we have a lot of smart people working for us, but we get drawn in with this cool factor and throw it over the wall and just assume that the guys in field are going to know what to do with it.

  - *What are the procedures, requirements, and decision points that are used?*
- *How do requirements for information sharing systems drive training requirement for newly arriving personnel?*

Well, they should be driving training but they are not in the way that they should be. My understanding, unfortunately, is that most of the training that is provided these days is nothing more than button ology. We are very scarce on decent operational training. What I mean by this is: we teach people what is on each screen, and what functions you can get by pushing buttons X and Y. What we don’t do, and should do, is say – here’s what your job is. Let’s take some operational scenarios, and we’ll show you how to integrate this new equipment so that you can do an even better job. We need training that is based on Watch stander procedures – and how those procedures will CHANGE, and how to get the information they need from the new equipment. Unfortunately, the poor watch standers are left to figure that out themselves … and a lot of otherwise useful functionality is ignored, because no one showed them how to integrate it into their jobs.

4. *With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?*
   - *Ease of use?*
   - *Desirability (of wanting to use the system)?*
     Usefulness?

Not too much as far as I can tell; at this point, I need to let you know some of my bounds here, over at the R&D Center with the exception of Rescue 21 and the Hawkeye system, I have not been part of an actual acquisition. We are usually up front looking at prototypes or thinking about capabilities, but once it rolls up into a real acquisition, it goes to a whole different project group at headquarters and people in CG-1B3 that was only stood up about three or four years ago are now the human factors folks that are actually responsible for acquisition projects. From projects that I have seen, human factors are not considered very much. A piece of that is that when we have centers such as C2CEN, who know the technology backwards and forwards, they become “too expert” and thus build something that works for them and they don’t really think about who the eventual user is going to be. Just little things like getting them to change the lexicon so that it is Coast Guard operational words and not computer science words are surprisingly difficult. Rescue 21, (I guess that it is ok to talk about that now because the system has been totally revamped), had something like seventeen to twenty button pushes to get sensitive, time-critical information into Rescue 21. Well you may have this poor person sitting there waiting to be rescued, on the radio, trying not to drown while talking to you, and we saddled our people with that kind of difficult-to-use system at the point that it went through OT&E. Fortunately our senior commanders said no way are we going to go anywhere with that system until it has been greatly improved. However, I have not seen it since it has gone through its final reworks, but that was a system that was acquired, human factors was written in the contract requirements but obviously the contractor did not have Human Factors personnel on its team. Had Rescue 21 been acquired today, 1B3 would have stepped in and fixed the problems way before OT&E. Rescue 21 technologically is a sound program that does things we never before imagined with ease, which is lovely, but it was not done in a way that made it helpful to the operator. One example of the poor user interfaces and system lacking integration was Rescue 21 into the Command Center equipment suite – a process the watch standers called "sneaker net." In order for the communications watch stander to get certain information over to the Ops guy, he had to write it out to a CD and run it over to Ops because they did not have any way of marrying Rescue 21 system with SarOps or anything else other equipment in the Command Center. It Rescue 21 just was not constructed with the users in mind; it came more from the technological point of view.

5. *In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?*

What kind of information are we talking about here? [Interviewer provided a scenario of intelligence that the Coast Guard had of a wanted fugitive on a commercial ship pulling into Boston Harbor, how could we improve that exchange and keep sensitive information from falling into the wrong hands.] What hits me first is that the agencies need to come-together first and discuss each one's needs so that we understand how certain kinds of information may be very important to us but not be so important to another agency. If that other agency comes across that information and they are aware that it is very important to us, then they may be more willing to share it or maybe think that it is something to share. Thus, I think from an organizational point of view, if we understand the kind of the hot buttons of our brother and sister agencies that may be a good starting point. With respect to sharing information with the public or the maritime community the thing that comes to mind is something we learned while doing a Western Rivers project a couple of years back. We asked mariners what they did if they noticed buoys off station or problems in the waterways. We found out that people on commercial vessels moving up and down the Mississippi don't even report this stuff any longer because they know that nothing will be done about it by the CG, or nobody from CG ever gets back to them about it when they do report something. So they have no idea if the information that they pass gets acted on or will be acted on. It seems like it is something that could be done fairly easily with all of the interactive mapping tools that we have at our disposal. One could potentially put something onto an ECDIS (electronic chart) that indicates that "yes we know this buoy is off station, it will be fixed in a couple of months or we have somebody coming down river to check on it" I think that this was workload issue for the Coast Guard but I don't remember what the findings were.

4. Technical Director Interview

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.

- *Specifically, what challenges are encountered in information sharing between the public and private sector?*
  What are your top three challenges?

Ok, well I think what we have found in our maritime domain awareness data sharing community of interest, when we started that project we really focused on data sharing and we found that data sharing really was not the issue. We started with the Automatic Identification System (AIS) information system and several agencies had AIS information in databases: the Navy had some, DHS had some, and the Coast Guard had some. There also was the NAIS major acquisition, they all had information, and they wanted to share it. So we thought, ok, well, let's get some unclassified AIS and put it on the net centric enterprise service program which was the DISA portal and let's go ahead and share that among agencies. So, that wasn't actually that hard in that what they had to do was take the different ways the information was represented and what type of status schema each of them was using, get together and agree on a common schema. Once they agreed on a common schema and they wrote it in XML, then everyone who had a proprietary data set, simply had to develop a wrapper to translate the data from that common schema. When you were a publisher, you would publish on the NCIS data bus, and then a subscriber would subscribe to it, in that common format and then translate back to their proprietary format. That actually was relatively easy, but, even with unclassified AIS information, which we thought would be our most useful data set to manipulate, we found out that the unclassified set of data that the Navy intelligence program had was still sensitive because it came from commercial shipping companies and those commercial shipping companies did not want their competitors to have information on where their ships were. Mostly because their competitors could use that information for competitive advantage. So, what we had to do was figure out a way to safeguard that information. We started by just having a special channel for that but that kind of defeated the purpose of information sharing. So we spent the next three years investigating different ways to secure information when it is in a public in a subscription type format. In the three years that we were engaged in that activity we never actually found a technology that did that for us, because even if you would secure it as you placed it on an enterprise service bus, the publisher did not have any assurances that the information would not get into the wrong hands somewhere down the road. So that was actually the biggest challenge that we had been securing access for the data sharing. That is really, what your thesis is about information assurance. I left however and I sort of lost track of it. If you can get down to SPAWAR and you look into crypto binding you should be able to see what sort of success they had there. It was not classified technology but it was encryption because what they would do is encrypt the data and wrap it in an encrypted layer that would stay with that information throughout its life cycle. I am not sure where that ended up going as I changed jobs and lost touch with it. Mr. Green was the gentleman's name and he could update you on the technology but that was the most promising technology that we found for securing the information.

2. What is the method used to design and/or select Command and Control (C2) systems to share information?

- *What are the procedures, requirements, and decision points that are used?*
- *How do requirements for information sharing systems drive training requirement for newly arriving personnel?*

Well, it is really in acquisitions which really everything is. Federal acquisition policy regulates the process on that so really in the Coast Guard and DHS, the Coast Guard has a Major System Acquisitions Manual and DHS has the Systems

Engineering Life cycle which is very similar in process for starting with documenting the need, and identifying the capability gap, then generate the requirements document, the award, then go perform the market research, research and development, prototyping, then issuing the request for proposal and nine times out ten it is going to be a commercial acquisition where you are going to allow the private sector to develop the solution and compete against each other. So you do the request for proposal then you do the source selection, then you go through the protests, write the contract and they start developing that solution for you. The most important aspect is that the sponsor remains engaged throughout the entire process i.e., the sponsor starts it, the sponsor works with research and development, the sponsor works with the acquisitions community, the sponsor works with the contracting community, the sponsor participate in selection, the sponsor makes sure that the resources are available for all phases including O and M and disposal. A lot of times when you start down the SDLC, SELC, or the MSAM there are so many requirements for review and documents; people forget to walk along with the other people that are attached to that process. Typically what you have is a contractor in California and you are somewhere on the East Coast and from headquarters that is difficult to keep track of. That is about the best answer that I can provide in terms of how it is to be done (following the acquisition process) otherwise you end up getting so far down the road and a protest comes along and wipes out the whole thing and you are back to square one.

One of the best things that I witnessed (surprisingly you do not see this very often) at the Navy research lab that were doing their vessel tracking project they were doing something called user juries that consisted of every three or six months I am not exactly sure what the interval was they would fly Coast Guard and Navy People in from different watch centers and sit them down in a room with the technology and have it linked to all these different data feeds and have them run through scenarios and give them comments over the couple of days that they lasted and that was a very good way of doing that. They were using a spiral development process at the time which allowed them to get really good feedback from the users while they were using the technology.

3. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?

- *Ease of use?*
- *Desirability (of wanting to use the system)?*
  Usefulness?

That really varies by the system, one of the real reasons that the R&D program was brought into the acquisitions directorate in Commandants Intent Action Order (CIAO) one which was one of ten reorganization proposals for modernization was to get the expertise in human factor into the front end research of the acquisition process. The R&D center did an analysis of rescue 21 program in its early days and gave it some good feedback on the way that the windows were structured. So they had a lot of human factors looked at through Dr. Blue was the human factors expert at the R&D center than while I was there. But this was before R&D was brought into the acquisitions directorate. Whereas, now, since I have left they are probably engaged more at the front end of acquisitions for the technology/human aspect of building a technology.

4. In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?

Like I said, I think that the challenge was being able to safeguard the data in a public publish and subscribe environment. So, I think if we had, in my belief was that in the three years that we did the project data sharing community of interest project, the belief was that was going to be handled in one policy. So, they stood up a policy group, and for three years the policy group could not solve that problem. They even got lawyers involved who (very competent and enthusiastic lawyers) were involved and when they started they said if we will just come up with a policy for this data sharing so that everybody knows who they can share with and who you could not share it with. This didn't work either. At the end of the project, I concluded that it had to be a technology solution not a non-material solution there had to be a way… You were in radio navigation, you were working with FAA, you worked with them in Loran and you work them in GPS all the time. The FAA is very careful about how many nines they assign to a safety and security so they will say they will design this to five nines (99.99999% availability.) The FAA, they would calculate that, so you would give them a technology or you would give them the probability scenario and they would calculate the number of nines for an accident in the air. That information would be used to build the system, the necessary redundancies for the system, the specification for the system, and that would be a level of confidence that a passenger would have in flying in that system. My conclusion was that it had to be a technology solution and there had to be an independent body that calculated an assurance level to several nines. One that had the power to say ok, if you implement this technology you would have 3 nines of security that you information is not getting into the wrong hands. If you needed four nines than you would have to use this, five nines this, sort of like the AES encryption thing where depending on how sensitive the data is you would use a different encryption method. Some of these choices may gobble up a lot of bandwidth, or one that costs you a lot for really sensitive data. So, I was just kind of thinking (PGP) Pretty Good Privacy is good enough for this data, I just want to make sure that this picture does not get on the Internet. So you had to have the independent body like SPAWAR has that crypto binding that they used the NSA as their independent board who is really the gold standard in information security. So, I liked that aspect of it. In a perfect world, you don't even need information assurance; you would only have to care about sharing. Alright, now the thing that is interesting is that in the JWICS system when you have the SCI information on the JWICS, they actually close the whole system.

So you share within the system but you don’t share with port partners, you don’t share with OGAs and you don’t share with your international partners. Or, you can do it point to point. So when you are talking about the GENSER system or the JWICS systems they close the system off and they assure information that way. When you are talking about unclassified data you are talking about dealing with port partners, you are talking about dealing with OGAs and international partners in the unclassified environment, it is a lot harder to safeguard the information then it is when you just close it off and you only give it to people who are cleared and have the need to know. I think that in the imperfect world if we could get to the point where we have a technology solution that was certified by the NSA to provide such different levels of assurance for such different levels of sensitivity that I think that we could unlock the information sharing world. That is what I think that we need, because you have to assure the publisher that their information will be safe before they will publish. That is the key; not data sharing itself so much as data security as exemplified perpetuated by confidence that one’s information will only be viewed by ones intended audience.

Push data is a topic of great interest in contrast to that I witnessed in data sharing communities of interest was that it was a pull type system. It was ok, let’s see what information is out there, which is Internet type of stuff, you can look up something on a webpage and get no information. There are several search engines that illustrate this; all that it does is display the title the engine page until you give it constraints to search from that the system engages and searches the World Wide Web for matches. Thus, a discovery and retrieval, then you are not overloading the user. There is the whole other aspect of that where you have automatic systems automatically going out and retrieving information that can be analyzed which is data fusion. One of the customers of the Coast Guards R&D Center indicated that “I don’t need more information, I need information fusion” Like the tools that is the Naval Research Center’s vessel tracking system was (an information fusion system.) They actually installed it at MIFICLANT and I think MIFICPAC and it is probably still in MIFICLANT.

5. Systems Manager Interview

1. As a governing agency leveraging many information sources, please describe your challenges in receiving and distributing that information.

The biggest challenge, (if I had to put it in a nutshell), for receiving and distributing information would be the quality of data that we are able to pull in from the various information systems that are out there. This kind of indicates another problem in that the sources that are out there are numerous and present a challenge for our operators to categorize into functional areas. This diversity of stovepipe type systems requires our personnel to dig into each source and develop a means to warehouse it, then tap into that information and manipulate it at as they see fit based on the algorithms that will drive a decision or solution set to get where they are going.

Specifically, what challenges are encountered in information sharing between the public and private sector?

That is a really good question from my perspective or a difficult question because we don't interface with the public too often as much as they do individual members of the service. This question is not really relevant to me. In terms of my previous experience though as a Lieutenant he had a job with the maritime domain awareness in regards to information sharing stuff when he interfaced with the public. One of the biggest challenges we faced was getting everybody into the same room and getting them to agree on what types of information needed to be collected or acted on, because different things are important to different groups of people.

What are your top three challenges?

[So, would you rank quality of information as the top or do you have a ranking of your challenges] From my current perspective in the CGBI staff I would say absolutely, when we go out and speak to like a sector staff, we are always getting pushback on every single visit that they make, it's "Hey, you know I went into your system, and I saw this or you guys told me this and that is not the case or this is not true. Why are you reporting bad information?" I literally have to stand there and say ok, I can look into this for you but I can't change what is being reported because at the end of the day I am pulling from a system that already exists (a system of record) that someone else is in charge of… This is an example of what makes quality of information such a big deal from my perspective. Because we have to go back to those system owners and data managers and ask about their internal quality control measures and how that information comes into existence. There is also an element of reminding those system owners that they are not the only ones to look at that data so more effort needs to be applied to fidelity. Also making sure that they know the information has utility outside of their systems or warehouses where it is making spread sheets. A lot of times the people that are developing these systems or an initial data set are the ones that will be the greatest users of that information. It is an illustration of the light going on when they recognize the customer is trying to hold them accountable.

One of my observations has been that when IT designs systems one of their focuses is to get as much information to the end-users as possible. Then leaving it to that end user to figure out exactly what it is that they need to make their decision. When the reality is that the specific information that they need is a lot less than what that IT person thinks of when they are diagraming user needs and so they are simply overwhelmed with information. Usually the answer that end-users need is there but they have to go digging for it.

2. What is the method used to design and/or select Command and Control (C2) systems to share information?What are the procedures, requirements, and decision points that are used?

I'm going to be honest with you, when the program first started, the methodology was: What is available? Who will talk to us? What can we actually pull into our enterprise data warehouse? That is really what happened, and that was ok for the initial phase. The next phase being, now we have this information, what can we do with it? As we were able to do that, it ended up becoming more of a proof of concept; like "look at all the neat, cool things that we can do, pull data from this group, that group, and the group over here, with which we created this really nice product. Then after creating this product and doing this proof of concept, we were able to go back out and say ok, now you see how this system works, we can now do this for systems that you are interested in Commander or Admiral. Won't you please work with us; and we will develop the system to satisfy your needs. That was the initial approach that we took, so as far as an initial methodology, I guess you might say it was a proof of concept based on any information that you were able to collect (with little attention given to human factors.)

How do requirements for information sharing systems drive training requirement for newly arriving personnel?

Well in theory the needs of the training requirement should be the guiding principle behind the development of the information sharing system because the whole point is to get the information to the people that use the system. In reality, I think what happens is again once we have something in place we tend to train to that with little attention given to what is needed. And what is needed tends to come after based on the training that is given. So, our folks, what they will do is go out and say ok this is CGBI, this is what it looks like, these are the systems that we pull from and we will actually show in our opening presentation all of the systems that we pull from. We may also speak a little bit to the types of information that comes from those systems. Then we will go into the various cubes and reports and products that we have and demonstrate how we manipulate some of those data sources to meet our needs and glean information based on the data that we are pulling into our own enterprise data warehouse. What happens after that is the folks that are being trained will come back to us and they will say "hey this was really cool and I liked your training, but what I really need is to see information that is coming from this system of record and I did not see that system listed in the slide presentation that you did. So, how do I go about getting this system of record listed and also once I get it listed I would like to know how to build measures that will help me take advantage of the information that I will be pulling from those systems of record once it is added?" For this we have an actual measures division if you will and they will go out and sit with the client and build metrics that help determine the value of the information they are providing to the client. So, they are as responsive to client needs as possible, but often what the client has a mental picture of as a system of record is not really a system of record and they will try to work with them and see if we can get the system they want into CGBI by steering them toward an actual system of record or steer them down a path to building their own system. We will even do things like try and help them to develop something like a flat file and pull that into the OSC enterprise service bus. Sometimes we can do stuff that way, that is not always the case, it just depends on resource availability. The best way to deal with this sort of thing is to get information into an actual system of record, but sometimes a client just can't do it, or there is nothing available to support them and we end up having to tell them no. We try not to do that, but that is sometimes the reality and there is just nothing that we can do for them.

3. With regard to information sharing, to what extent are human factors considered in the selection of a potential C2 system, such as?

- *Ease of use?*

- *Desirability (of wanting to use the system)?*
  Usefulness?

CGBI is not in the business of selecting new systems; however, they are in the business of trying to improve the ones that we have. When it comes to human factors driving what we do, I would say very much so. Because one of the things that our current flag officer is really, really good about (and we are excited that he is) because it means funding us is the idea behind our system. He came out and said "Look, you know this is a great product that you guys have, but, the thing is that when folks go to use it, there is this heavy lift on the training side, there is a heavy lift in exactly what you can get from this system. I need you to make it easy, I need the one click, two click solution." So it would appear that human factors are going to be shaping our acquisitions and development for much of the foreseeable future and how existing systems such as CGBI will be upgraded in the future. We are working on this thing now called CGBI 3.0 and one of the things that we are looking to do is literally make it easier to use weather that be place tickers on the bottom of the screens, or e-mail notifications that the user has to pull out, or RSS feeds. So human factors are critical and they will continue to be shaping future Coast Guard systems. Another characteristic of Coast Guard is systems are that they are generally the product of a single persons idea of a great system and where I am going with this is a person gets tasked with looking into something and they build a little system of their own that is functional for that need. Someone will see that setup and voice it that it should become an enterprise system output when that is almost impossible to achieve. Then the person who had the idea originally has been reassigned or moved on and the service has this massive system trying to implement their idea. This situation tends to highlight the importance of making people document both their thought process and how they implement things.

4. In a perfect world – without any constraints - how might information sharing be improved within the Coast Guard?

What I would say or what I would do is try to improve the governance section and not only control what units are allowed to purchase IT equipment. Finally, A focus on passing knowledge, enforcing standardization, and holding people accountable for their actions would take us long way.

LIST OF REFERENCES

AOPA ONLINE (n.d). *History and Mission of AOPA* Retrieved from AOPA'S MISSION: http://www.aopa.org/info/history.html

AMERICAN Public Transportation Association. (2012). *About APTA*. Retrieved from General Information: http://www.apta.com/about/generalinfo/Pages/default.aspx

BOSTON Pilots (2012). *Boston Harbor Pilot Association*. Retrieved from Welcome: http://www.bostonpilots.com/

Bencoma, L. A. (2009). Modeling the effects of a transportation security incident on the commercial transportation system. Monterey. Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2009/Sep/09sep%5FBencomo.pdf

Burke, K. (2007). The Commonwealth of Massachusetts State Homeland Security Strategy. Boston, MA. Retrieved from: http://www.mass.gov/eopss/docs/helpus-helpyou/state-homeland-security-strategy-092307.pdf

City of Boston. (2012). About Boston EMS. Retrieved from www.cityofboston.gov/ems

Commonwealth of Massachusetts. (2012a). Official website. Retrieved from Mass.gov: http://www.mass.gov/portal/

Commonwealth of Massachusetts. (2012b). Public Safety. Retrieved from MEMA Mission: http://www.mass.gov/eopss/agencies/mema/

Commonwealth of Massachusetts. (2012c). Fusion Center Overview. Retrieved from Public Safety: http://www.mass.gov/eopss/home-sec-emerg-resp/fusion-center/fusion-center-overview.html

Commonwealth of Massachusetts. (2012d). massDOT. Retrieved from http://www.massdot.state.ma.us/

Commonwealth of Massachusetts. (2012e). Mass.gov. Retrieved from Public Safety: http://www.mass.gov/eopss/agencies/msp/

Cudahy, B. J. (2006). *Box boats: How container ships changed the world.* Fordham University Press, New York, 1st.

Cung, V. (2012). *National Maritime Intelligence-Integration Office Technical Bulletin.* Washington, DC: ONI Media Services.

Department of Homeland Security Information Sharing Strategy. (2008, April 18). United States of America: United States. Department of Homland Security. Retrieved May 17, 2012, from https://www.hsdl.org/?view&did=486486

FBI.gov. (n.d. a). About Us. http://www.fbi.gov/about-us

FBI.gov. (n.d. b) Joint Terrorism Taskforce. http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs

Federal Aviation Administration (2010, April 4). About FAA. Retrieved from Mission: http://www.faa.gov/about/mission/

Government Accountability Office. (2010a). *Information sharing: Federal agencies are helping fusion centers build and sustain capabilities and protect privacy, but could better measure results: Report to congressional requesters* [electronic resource].

Government Accountability Office. (2010b). *Supply chain security : CBP has made progress in assisting the trade industry in implementing the new Importer Security Filing requirements, but some challenges remain: Report to congressional requesters*.

Government Accountability Office. (2010c). *Supply chain security: DHS should test and evaluate container security technologies consistent with all identified operational scenarios to ensure the technologies will function as intended : Report to the Chairman, Committee on Homeland Security* [electronic resource].

Grillot, S. R. (2010). *Protecting our ports domestic and international politics of containerized freight security*. Burlington: Ashgate Publishing Company.

Grimes, J. G. (2007). *Department of Defense Information Sharing Strategy*. Washington DC: Department of Defense. Retrieved May 17, 2012, from https://www.hsdl.org/?view&did=480172

Irvin, L. (2002). *Not yet all aboard...but already all at sea over container security initiative*. Singapore: Institute of Defence and Strategic Studies Nanyang Technological University The Republic of Singapore.

ISE. Information Sharing Environment (n.d.) About ISE. Retrieved from What is ISE?: http://ise.gov/what-ise

Larence, E. (2007). *HOMLAND SECURITY federal efforts are helping to alleviate some challenges by state and local information fusion centers*. Washington, DC: United States Government Accountability. Retrieved 2011

Levinson, M. (2006). *The box: How the shipping container made the world smaller and the world economy bigger*. Princeton University Press, Princeton, N.J.

Marie, C. &. (2010). *Arctic Region Policy Information sharing model options* (master's thesis). Naval Postgraduate School. Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2010/Sep/10Sep%5FMarie.pdf

Massachusetts Bay Transportation Authority. (2012, May 15). Massachusetts Bay Transportation Authority. Retrieved from MBTA: http://www.mbta.com/

Massport. (2011, August 29). MASSPORT. Retrieved Aug 29, 2011, from Massport: http://www.massport.com/port-of-boston/About%20Port%20of%20Boston/AboutPortofBoston.aspx

Massport. (2012, May 20). MASSPORT. Retrieved from About Massport: http://www.massport.com/massport/about-massport/Pages/AboutMassport.aspx

MDA.gov (2012). The Maritime Domain Awareness Information Exchange. Retrieved from About: http://www.mda.gov/about/

National Maritime Domain Awareness Coordination Office. (2012, May 18). NMCO vision: http://www.gmsa.gov/about.html

National Maritime Intelligence-Integration Office (n.d.). About NMIO. Retrieved from Our Mission: http://www.nmic.gov/aboutnmio.htm#missionNational Strategy For Information Sharing Successes and Challenges in Improving Terrorism-Related Information Sharing. (2007, October). Washington, DC. Retrieved from http://ise.gov/national-strategy

Nedrix. (2012, May 20). *NEDRIX*. Northeast Disaster Recovery Informaiton X-change: http://www.nedrix.com/

Network, A. P. (2012, May 20). *APAN*. Our Mission: https://community.apan.org/p/about.aspx

Passenger Vessel Association. (2007). Passenger Vessel Association. Retrieved from About PVA: http://www.passengervessel.com/about.aspx

Rinaldi, L. J. (1972). *Containerization: The new method of intermodal transport.* New York: Sterling Pub.

RISS Regional Information Sharing System (2012). RISS. Retrieved from Mission: http://www.riss.net/Default/Overview

RITA. (n.d.). Vision and mission. Retrieved from http://www.volpe.dot.gov/about/mission.html

RITA (2011). *John A. Volpe National Transportation System Center* Retrieved from Welcome to Volpe Center: http://www.volpe.dot.gov/about/index.html

Salem, A. H. (2011). Port of Boston industry and public sector cooperation for information sharing. *MIST Multimodal Information Sharing Team* [Unpublished Manusript].

U.S. Department of Homeland Security. (2009, Feb 17). *CBP Mission Statement and Core Values*. Retrieved from CBP Mission Statement and Core: http://www.cbp.gov/xp/cgov/about/mission/guardians.xml

U.S. Department of Homeland Security. (2011, July 25). *Department of Homeland Security Information Sharing Strategy*. Retrieved from Information Sharing Strategy: http://www.dhs.gov/files/publications/gc_1212068752872.shtm

U.S. Department of Homeland Security. (2011). Ten years after 9/11: A report from The 9/11 Commision chairmen. Monterey: Naval Postgraduate School.

U.S. Department of Homland Security (2012a). *United States Coast Guard*. Retrieved from Acquisition Directorate: http://www.uscg.mil/acquisition/ioc/project.asp

U.S. Department of Homeland Security (2012b). *Transportation Security Administration*. Retrieved from Layers of Security: http://www.tsa.gov/what_we_do/layers/index.shtm

U.S. Department of Homland Security (2012, Jan 26). *United States Coast Guard*. Retrieved from Missions: http://www.uscg.mil/top/missions/

U.S. Department of Homeland Security. (2012, Mar13) FEMA. Retrieved from About FEMA: http://www.fema.gov/about/index.shtm

U.S. Department of Homeland Security. (n.d.a). Homeport U.S. Department of Homeland Security United States Coast Guard. Retrieved from Boston: https://homeport.uscg.mil/mycg/portal/ep/programView.do?channelId=-17385&programId=12608&programPage=%2Fep%2Fprogram%2Feditorial.jsp&pageTypeId=16440&BV_SessionID=@@@@0209741447.1337565009@@@@&BV_EngineID=ccccadfgkekgklkcfjgcfgfdffhdghj.0

U.S. Department of Homeland Security. (n.d.b). Information Sharing. Retrieved from Information Sharing : http://www.dhs.gov/files/programs/sharing-information.shtm

U.S. Department of Homeland Security. (n.d.c). About ICE. Retrieved from Overview: http://www.ice.gov/about/overview/

U.S. Department of Homeland Security. (n.d.d). Secretary Napolitano Announces Rail Security Enhancements, Launches Expansion of “See Something, Say Something” Campaign: http://www.dhs.gov/ynews/releases/pr_1289842248570.shtm

U.S. Department of Homland Security (n.d.e). Missions. https://homeport.uscg.mil/mycg/portal/ep/home.do?tabId=0&BV_SessionID=@@@@0370423123.1337560724@@@@&BV_EngineID=ccccadfgkihmmjjcfjgcfgfdffhdghm.0

U.S. Department of Transportation, (2012, March 27). About DOT. Retrieved from What We Do: http://www.dot.gov/about.html#whatwedo

U.S. Department of Transportation Maritime Administration (n.d.). Maritime Administration At A Glance. Retrieved from About Us: http://www.marad.dot.gov/about_us_landing_page/at_a_glance/at_a_glance.htm

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Captain John J. Macaluso
   U.S. Coast Guard
   Alexandria, VA

4. Commander Karl Davis
   U.S. Coast Guard
   Washington DC

5. Commander Paul Arnett
   U.S. Coast Guard
   Boston, MA

6. Jay W. Spalding
   U.S. Coast Guard R&D Center
   New London, CT

7. Dr. Anita Rothblum
   U.S. Coast Guard R&D Center
   New London, CT

8. Dr. Doug MacKinnon
   Naval Postgraduate School
   Monterey, CA

9. Dr. Danial Boger
   Naval Postgraduate School
   Monterey, CA

10. Glenn Cook
    Naval Postgraduate School
    Monterey, CA

11. Lieutenant James Ware
    U.S. Coast Guard
    Juneau, AK