Maritime Operational Information Sharing Analysis

September 2014

Prepared by the Department of Human Centered Design & Engineering
at the University of Washington

Prepared for the Department of Homeland Security Interagency Operations Center,
the National Maritime Intelligence-Integration Office, and
the Program Manager for the Information Sharing Environment

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY INTERAGENCY OPERATIONS CENTER, THE NATIONAL MARITIME INTELLIGENCE-INTEGRATION OFFICE, AND THE PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT, BY THE UNIVERSITY OF WASHINGTON DEPARTMENT OF HUMAN CENTERED DESIGN & ENGINEERING

MOISA.COM

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

First printing, September 2014

TITLE PAGE IMAGES

Larry Ehl. (2011). "Port of Tacoma - Evergreen Terminal." www.transportationissuesdaily.com
Howard Garrett. (No date.) "Orcas Swimming near a Washington State Ferry." www.globalgiving.org
USCG Petty Officer 3rd Class Colin White. (2009). "Bertholf Arrives in Seattle."

ACKNOWLEDGMENTS

The University of Washington acknowledges the contributions made to the research and publication of the Maritime Operational Information Sharing Analysis Report. We would like to thank the Puget Sound maritime community for their continued support throughout the project. Specifically, we thank the:

- Marine Exchange of Puget Sound and Captain John Veentjer, U.S. Coast Guard, Retired, Executive Director
- Captain Scott J. Ferguson, U.S. Coast Guard, Retired, Sector Puget Sound Captain of the Port (2010-2014)
- Captain M.W. Joe Raymond, U.S. Coast Guard, Sector Puget Sound Captain of the Port (2014-Present)
- Marvin Ferreira, Security Manager and all employees of APM Terminals Tacoma
- Military Surface Deployment and Distribution Command (SDDC)
- Area Maritime Security Committee (AMSC), Puget Sound
- U.S. Coast Guard, Sector Puget Sound
- Marc Mes, Maritime Security Director, Canadian Coast Guard
- Canadian Coast Guard Maritime Communications and Traffic Services (MCTS) Western Region: Brian Bain, Superintendent; Ian Wade, Regional Program Specialist; Clay Evans, SAR Superintendent; and Lindsey Funk, Operations
- Marine Security Operations Center (MSOC): David Dahlgren, Lead Officer; Marc Hahlen, Maritime Security Officer; and Lorna Cameron, Maritime Security Officer

We would also like to thank the sponsors for their support and contributions as partners in this project.

- Department of Homeland Security Interagency Operation Center
- National Maritime Intelligence-Integration Office
- Program Manager for the Information Sharing Environment

MOISA CONTRIBUTORS

Undergraduate Students: Emma Bulajewski, Morgan Duffy, Heather Eberhart, Stephanie Lynn Grose, Perry Meas, and Anu Mohajerjasbi

Graduate Students: Melissa Braxton, Dharma Dailey, Trevor Johnson, Michael McLeod, Pam Munro, and Maura Rowell

Consultants: Christena Little and Anne Tyler (CDR, USN Retired)

PI Team: Dr. Keith Butler, Dr. Mark Haselkorn, and Dr. Mark Zachry

Contents

List of Figures

List of Tables

Executive Summary

The Takeaway

Year one of the Maritime Operations Information Sharing Analysis project (MOISA1) was a descriptive, ethnographic exploration of the complex daily operational information sharing environment (ISE) of the Puget Sound security and safety community (PSSSC). MOISA1 revealed fundamental information with profound actionable implications for the security and safety of our country. These implications include:

1. A critical need to refine how we identify, conduct, deliver, and maintain initiatives designed to enhance regional security, safety, and resilience
2. Insights into community-based strategies to increase the immediate and long-term value of these initiatives, particularly when they are based upon use of information and communication technologies

On a daily operational basis, the PSSSC's ISE is extremely effective, yet it is also highly informal, based largely on knowledge of people, organizations, and work practices (community self-knowledge) and communities of trust that continually evolve through ongoing relationships and shared experiences. Aside from generic communication technologies such as phone and email, past investments in security IT systems have not had a major impact on the community-wide ISE in any way proportional to the size of those investments. This primarily results from a critical misalignment between, on the one hand, the funding, design, development, implementation, and maintenance strategies of Federally-funded IT security initiatives, and, on the other hand, the work, information sharing environments, and mission performance of the people and organizations charged with the daily security and safety of their region. This mismatch between the strategies and practices of IT initiatives and the ISE of the regional operational community doom these initiatives to limited, if any, long-term value.

Rather than simply point out the current lack of impact of regional security IT investments, MOISA1 also points towards approaches and methodologies that can align future federal security and safety IT investments with the ISE within which those investments must live and thrive. If we base future ISE initiatives on the successful ways people currently work and share information to accomplish their security and safety missions, and if we cultivate community-ownership of these initiatives, they will sustain and grow, providing long-term benefits even beyond those for which they were initially intended.

The ISE of Daily Operations

Post-9/11, our Nation has focused on information sharing to address major incidents. Through a massive effort we have established incident management standards and enhanced our nation's ability to coordinate responder activities. But security and safety are not just incident-based endeavors; they are also services that must, like power and transportation, be operational 24/7 in support of economic resilience and societal well-being. A comparable effort is needed, focused on daily multi-agency operational information sharing and integration.

In 2013, three Federal agencies joined together to initiate such an effort: (1) the DHS Interagency Operations Center (IOC) led by the U.S. Coast Guard, (2) NMIO - "the unified maritime voice of the United States Intelligence Community (IC)"[1] and, and (3) PM-ISE - established in the White House after 9/11 to promote "national security through responsible information sharing."[2] This partnership was driven by a recognition that resource allocations, policy decisions, and technical solutions intended to improve security, safety, and resilience needed to be based on a better understanding of the daily operational information sharing practices, challenges and requirements of the diverse security and safety community.

MOISA1 was a collaborative effort with the PSSSC to answer the question: What is the nature of the community's daily operational ISE and what is the role of that ISE in achieving their collective missions? The community's answer, repeated many times in many ways, was simple and nearly unanimous: "When it comes down to it, it is all about relationships." While the maritime community's focus on trust relationships, and the ability of these relationships to support highly nuanced information sharing, may sound unrelated to state-of-the-art technology-based security initiatives, these initiatives wrestle with the same issues of trust and information access, *e.g.*, identity and entitlement management. Furthermore, these technology

[1] United States Navy. National Maritime Intelligence-Integration Office. (2014). What is NMIO? Retrieved from nmio.ise.gov

[2] Program Manager, Information Sharing Environment. (2013). Information Sharing Environment Annual Report to the Congress: National Security through Responsible Information Sharing.

"solutions" are dependent upon acceptance and use within the community's operational ISE for sustained existence and meaningful impact.

PSSSC members work on a daily basis to achieve self-knowledge of their diverse and dynamic community, and to align their ISE with the work they do in support of their missions. They view the quality of this trust-based, largely self-organized ISE as a key element of regional resilience in the face of threats to security and safety. Even during incident response, the National Incident Management System (NIMS) relationship framework does not replace the importance of the extremely rich and nuanced, informal community fabric of identity and trust. As the previous Captain of the Port put it, holding up his NIMS manual and introducing an earthquake exercise, "This is our going in position." Once an incident occurs, the community still relies on its ongoing fabric of trust to coordinate and innovate, perhaps even more so. The community views this ability to coordinate and innovate, based on the ISE that they have exercised and worked to improve on a daily basis, as their greatest asset.

The ISE of daily operations, however, is not the same as the ISE of incident response. We found that most members of the community do not on a daily basis see security as their number one job. Even a police interviewee identified his primary job as community relations. Daily operations occur at a different pace and focus than the intensity and time pressure of incident response. Daily operations are highly motivated by economics, including barriers to information sharing due to competition that are set aside during incident response. Yet despite these and other differences, the ISE of daily operations and incident response are intimately intertwined.

While the PSSSC works hard to strengthen its relationship-based operational ISE, there are still some critical gaps. There are gaps from personnel turnover and retirement, from stove-piped thinking and investment, from conflicting priorities and missions and cultures. Where gaps exist, regional resilience is decreased. Gaps in the community fabric of trust and self-knowledge; gaps in the framework for information sharing; gaps in the understanding of who needs what, when, how and whether or not they should receive it; these translate into less effective and responsive action by the community. For this reason, the PSSSC invests significant time and energy in an ongoing effort to establish trusted relationships and maintain self-knowledge.

There are numerous formal systems in the Puget Sound region intended to receive, store, and deliver incident-focused information. The parts of those systems that come closest to acknowledging the daily operational work of the community are identity and entitlement management — who are you, can I trust you, what can I appropriately share with you? In terms of systems design, formal methods for identify and entitlement management are a major focus of national initiatives to improve the ISE, but these formal methods are far less of a focus of the diverse regional community. The PSSSC shows little interest in or awareness of data standards or meta-tagging or national exchange models. This is likely because they are working on a daily basis to maintain a nuanced and non-technology based system of identify and entitlement management, focused on knowledge of people, organizations and work practices.

Initiatives to improve the regional ISE for security and safety need first to understand the existing informal ISE of daily operations. Federal-centric systems, delivered as a series of technology-based solutions, have not supported the daily work and mission of the community, nor have they supported the strengthening of community trust and self-knowledge. In the past, these systems have been brought in piecemeal with few plans for sustainability. They have added new, unplanned overhead work and made work harder, not easier. They have not been owned by the community as a whole, not designed based on a thorough knowledge of how the regional community works, how they share information, and how they self-organize. They have introduced constraints and had unintended consequences, addressed one problem of a complex, highly interdependent system (usually a problem of the Federal component) at the expense of introducing new issues elsewhere in the system (usually at the local level).

Yet despite years of attempting to accommodate a series of federal solutions; despite continually following directives that require the locals to put information into formal systems, with little or no reciprocal return of information of use to regional efforts; despite a Federal funding strategy that leads to fragmented and duplicative efforts with no long-term strategy; the regional community still looks to the federal component for support and guidance. The regional community still seeks rational policy and true partnership. Who else but the Federal government is in the position to provide it?

There are critical questions to be answered. What will it take to align federal investment in security and safety with regional work and practices to better provide security and safety for its citizens, institutions, and infrastructure? What will it take to gain community acceptance and ownership of future solutions and strategies? How do we design sustainable solutions and strategies that improve over time and with use, rather than degrade as they currently do?

In order for investments in IT security systems to meaningfully impact regional and national security and safety, these systems must be designed and implemented through methods that center on the people of the maritime community and their work. MOISA1 demonstrates an evidence-based methodology for achieving a more holistic, human-centered approach to enhancing security systems. This demonstration provides a rigorous process model of a container terminal's security-related cargo operations, and examples of the benefits that such a model can provide. While not the only approach, modeling gives insight into the benefits of basing future security system enhancements on a deeper understanding of the complex system by which that security is currently being delivered, as well as on a deep involvement of the community currently delivering that service.

Throughout the life-cycle of technology systems intended to enhance the regional ISE, designers, developers and sponsors need to incorporate the knowledge of the operations community to address the informal aspects of actual work as well as the formal assumptions of policy and procedure, the diverse daily operational environment as well as the centrally structured NIMS environment, the human and work needs as well as the technological constraints. Perhaps the long-term answer lies in an integration of the perceived but often false dualities of formal and informal work, of online technical activity and offline human activity, of daily operations and emergency response, of central and local. We can address these challenges more holistically, recognizing their existence within a wider, interdependent and dynamic socio-technical system. This is not easy, but there are emerging fields of human centered design and engineering dedicated to achieving this goal. These fields are given impetus by the growing realization, in the context of failures like Microsoft VISTA and the troubled healthcare system roll-out, that if you cannot afford the time and resources to do it right the first time, you certainly don't have the time and resources to do it over again. . . and again.

The Way Forward

THE way forward will require refining aspects of the current relationship between the federal and regional components of the FSLTIPP. To achieve this new relationship and new ways of enhancing the regional ISE, we recommend that appropriate elements of the Federal Government:

- Provide resources not only for initiatives that support incident response and management, but also support the continuum of daily operations that are critical to enhancing the ISE. These activities should be understood as a single operational environment, not competing activities.

- Leverage the current ways that the ISE is successfully established and maintained, *e.g.*, IT systems that support community trust building and self-knowledge.
- Employ project methods that address community identified opportunities for ISE enhancements and produce evidence-based, predictable improvements in security and safety mission performance.
- Base any ISE enhancement on a clear understanding of the work and information sharing environments within which the enhancements must live and evolve.
- Invest in regional community participation and leadership in the design of ISE solutions that will cultivate community ownership of these solutions.

These approaches will empower the regional security and safety community to play a strategic role in the design of their future ISE.

Potential MOISA-specific projects that could move this agenda forward include:

1. **Expand MOISA:** Conduct MOISA in other maritime regions; examine cross-regional best practices and the valuable similarities and differences among them.
2. **Expand Engagement with the Puget Sound Maritime Community:** Based on our year one results, expand the analysis of the current ISE, including expanding the interviewee pool and revisiting some entities.
3. **Develop and Employ New Capabilities for Coordinated Regional Assessment and Deployment of Potential ISE Enhancements:** Develop a regional test bed that demonstrates new methods for collaboratively improving the regional ISE.
4. **Apply Model-Based Design to Community-Identified Information Sharing Challenges:** For example, address an identified information gap between 9-1-1 and USCG SAR by working closely with practitioners to model the as-is work and information flow and produce an evidence-based improved to-be model representing a cost-effective solution.
5. **Explore Sustainability Issues:** Develop design strategies that enable the community to continue to adapt solutions after they are fielded.

6. **Region-Specific ISE Needs:** Explorecommunity-identified information gaps in the context of daily operational needs. For example:

   (a) *Radio interoperability* - analyze reported communication failures and support the community in identifying mechanisms for expanding regional radio interoperability that supports day-to-day mission accomplishment.

   (b) *Sensors and sensor data* - Support the community in developing an inventory of available regional sensor data and a plan for using that data in support of day-to-day operations.

   (c) *Situational awareness and common operational picture* - Support community assessment of the various SA/COP regional initiatives with an eye towards determining the desirability and feasibility of a single regional system for SA/COP that supports day-to-day operations and is used on a day-to-day basis.

   (d) *Essential Elements of Information (EEI)*- Support King-county led initiative to define regional technology-agnostic EEIs.

7. **Funding Alignment:** Examine federal funding practices and policies, with emphasis on understanding how community-based processes are valued. Explore with the community a collaborative mechanism for achieving alignment of federal, state and local investments.

8. **Explore Applications of MOISA to Federal Coordination Initiatives such as NIEM:** Explore how modeling the regional community's work and information flow can generate NIEM terms.

With these and associated steps forward, MOISA will play a critical role in ongoing efforts to develop and deploy long-term, sustainable enhancements to the operations that assure our nation's security, safety, and resilience. These enhancements will be based on a rich understanding of the partnerships and information sharing occurring every day across the diverse community charged with this precious task.

1 Introduction

> *Communities - either mission focused communities of interest, or professionally or technically focused communities of practice - provide a way to build coalitions and deepen relationships to mutual benefit. With our journey to accelerate responsible information sharing, the key is to bring together mission-focused and functional communities, and together to drive secure and trusted collaboration.*
>
> -Kshemendra Paul, Information Sharing Environment Program Manager, June 5, 2014

THE events of September 11, 2001 have dominated the U.S. perspective on national safety and security like no other event in our nation's history. This perspective has included a central focus on the critical role of information sharing and integration. As the 9/11 Commission Report famously put it,

> The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' No one component holds all the relevant information.[1]

Since 9/11, this desire to better 'connect the dots' has led to the establishment of the multi-agency Department of Homeland Security (DHS), as well as less visible but significant programs such as the National Maritime Intelligence-Integration Office (NMIO) and the Program Manager for the Information Sharing Environment (PM-ISE).[2]

Not surprisingly, the post-9/11 focus on information sharing has concentrated on major incidents, information to help prevent and prepare for, information to support response to, and information to help recover from those incidents. The massive effort to define, establish, and exercise a National Incident Management System (NIMS) has established incident management standards and enhanced our nation's ability to coordinate responder activities. But safety and security are not just incident-related; they are also services that must, like power and transportation, be operational 24/7 in support of economic resilience and societal well-being. The focus on major incidents has been necessary, but as a metropolitan Fire Chief put it,

[1] National Commission on Terrorist Attacks upon the United States., Kean, T. H., & Hamilton, L. (2004). The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States. Washington, D.C.: National Commission on Terrorist Attacks upon the United States. pg. 408.

[2] The PM-ISE also co-chairs the White House's Information Sharing and Access Interagency Policy Committee (ISA-IPC).

> I know more about what I'm doing the day after the earthquake than I know about what I'm doing tomorrow.

In order to maintain the needed level of ongoing safety and security, the time has come to direct a comparable effort toward day-to-day multi-agency operational information sharing and integration.

Safety and security in the maritime environment is one of the most critical components of national resilience and well-being. The United States is home to 361 ports hosting 700 ships a day and 8,000 foreign ships a year. The maritime transportation system provides employment for two million Americans and adds $700 billion to the U.S. economy.[3] Beyond the ports proper there are numerous other maritime activities such as domestic transportation (*e.g.*, ferries), recreational boating, military operations, tribal fishing, coastal refineries, and various maritime vessel services. And beyond even these are the numerous and complex intermodal interdependencies with land and air capabilities such as rail and aviation.

All these maritime related activities involve a large set of stakeholders from many sectors and levels of government. The resilience and well-being of our nation depend, in large part, upon the ability of these diverse stakeholders to share information on a day-to-day basis in support of effective collaboration.

In 2013, three federal agencies joined together to address these critical issues:

1. DHS Interagency Operations Center (IOC) led by the U.S. Coast Guard
2. NMIO – "the unified maritime voice of the United States Intelligence Community (IC)"[4]
3. PM-ISE – established in the White House after 9/11 to promote "national security through responsible information sharing"[5]

This partnership was driven by a common recognition that resource allocations, policy decisions, and technical solutions intended to improve maritime security, safety, and resilience needed to be based on a better understanding of the day-to-day operational information sharing practices, challenges, and requirements of the diverse safety and security community. The project came to be known as MOISA (Maritime Operations Information Sharing Analysis).

The Puget Sound region was chosen as the initial focus for MOISA for a number of reasons. The Puget Sound maritime community is a model of regional complexity with multiple ports, the largest maritime geographical area of operations in the United States, $33 billion in maritime commerce, the nation's largest ferry system, and a significant international border.[6] Puget Sound offers a unique

[3] Department of Homeland Security. (2008). Small Vessel Security Strategy.

[4] United States Navy. National Maritime Intelligence-Integration Office. (2014). What is NMIO? Retrieved from nmio.ise.gov

[5] Program Manager, Information Sharing Environment. (2013). Information Sharing Environment Annual Report to the Congress: National Security through Responsible Information Sharing.

[6] Community Attributes, Inc. (2013). Washington State Maritime Cluster Economic Impact Study. Prepared for the Economic Development Council of Seattle and King County and the Workforce Development Council of Seattle and King County with support from the Puget Sound Regional Council.

opportunity to analyze single and multi-agency information sharing processes, data, and technology and communication systems that support maritime operations across numerous federal, state, local, tribal, international, public, and private entities (FSLTIPP).[7] The University of Washington in Seattle was chosen to lead the MOISA effort.

This report presents the findings of the first year of MOISA, during which we worked with more than sixty regional agencies and organizations to describe and analyze day-to-day information sharing in support of safety and security of maritime operations. Engaging with regional stakeholders across the FSLTIPP, our goals were to understand the complex Puget Sound maritime information sharing environment and to explore possibilities for community-driven enhancements, as well as to begin modeling operational information flow as an integrated part of day-to-day workflow and mission accomplishment.

As we write this year one report, the continuation of MOISA into year two is already being planned. We plan to use the results, conclusions, and discussions presented here to support regional stakeholders in the definition and establishment of their future information sharing environment. Our goal is to provide evidence for and facilitate the establishment of a regionally co-designed information sharing environment — an environment based on a common understanding of effective community work practices and the day-to-day operations of trusted collaborations. It is these trusted collaborations that ultimately maintain the maritime security, safety, and regional resilience that we all continually rely on.

[7] "Public sector" and "private sector" are economic terms. "Federal", "state", "local," and "tribal" refer to government entities. Therefore, it appears that the term FSLTIPP is a composite of terms meant to differentiate different forms of government entities and economic arrangements.

2 Background

The Puget Sound region is geographically, economically, and strategically on the forefront of the maritime industry in the western United States. The Puget Sound is home to one of the most diverse and unique maritime communities in the nation. The maritime community of the Puget Sound[1] geographically encompasses the entire Pacific Northwest; it not only includes Washington State and Oregon but also Alaska and Canada to the north. The community is made up of a variety of stakeholders including but not limited to

- tribes[2]
- fishermen[3]
- recreational boaters
- tourists cruising up to the inside passage of Alaska[4]
- the largest ferry system in the U.S.[5]
- commercial shipping companies
- truck and rail companies
- safety, security, and law enforcement agencies
- the U.S. and Canadian Coast Guards
- the Federal governments of Canada and the U.S.

The international border between the U.S. and Canada is one of the most unique features of the Pacific Northwest waterways. The Strait of Juan de Fuca is a marine superhighway and requires a collaborative effort by the U.S. and Canada to ensure the safety of vessel traffic.[6] The Cooperative Vessel Traffic Service (CVTS), established in 1979, governs the waterway management of the Strait of Juan de Fuca and its connecting waterways.[7]

The Puget Sound not only refers to the northern waterways leading to the Pacific Ocean but also to the lowland areas surrounding the vast estuarine system. The Puget Sound stretches more than 100 miles and flows south through to Olympia. One beneficial feature is the naturally deep-water basins, the average depth being 205 feet.[8]

[1] The waterways east of the entrance to the Strait of Juan de Fuca, collectively referred to as the Puget Sound were officially designated by the USGS as the Salish Sea in 2009.

[2] There are 29 federally recognized tribes in Washington State. Governor's Office of Inidan Affairs. (2014). 2014 Centennial Accord.

[3] In 2006, non-tribal recreational and commercial fishing in Washington fisheries supported an estimated 16,374 jobs and $540 million in personal income. TCW Economics. (2008, Revised 2012). Economic Analysis of the Non-Treaty Commercial and Recreational Fisheries in Washington State.

[4] The Seattle cruise industry generates $381 million in business revenue and $16.8 million in state and local tax revenues each year. Community Attributes, Inc. (2013). Washington State Maritime Cluster Economic Impact Study.

[5] Washington State Department of Transportation (WSDOT) Ferries Division. (2014). Nation's Largest Ferry System.

[6] Both nations have navigational rights to the Strait. *Treaty Establishing the Boundary in the Territory on the Northwest Coast of America Lying Westward of the Rocky Mountains*, Washington, 15 June 1846, entered into force 5 August 1846 (The Oregon Treaty), *100 Consolidated Treaty Series* (C. Parry, ed.,) pg. 39-42.

[7] United States Coast Guard. (2013). The 2013 Vessel Traffic Service User Manual.

[8] NOAA. (2000) NOAA Technical Memorandum NMFS-NWFSC-44: Environmental History and Features of Puget Sound.

"Washington has the largest locally controlled public port system in the world with 75 port districts. The State has 2% of the U.S. population, and its ports handle 7% of the U.S. exports and 6% of all imports."[9] The Port of Seattle and Port of Tacoma combined are the third largest container complex in North America.[10]

The Port of Seattle (seaport)[11] located in the downtown Seattle urban center[12] was the 10th largest U.S. port in 2013 in terms of twenty-foot equivalents (TEUs) handled and the second largest in Washington State. The Port of Seattle specializes in container, grain, petroleum, and cruise ships. In 2013, the Port had 1,420 vessel calls and handled over 1.59 million TEUs.[13]

The Port of Tacoma, located just north of the downtown Tacoma urban center,[14] is one of the top 10 largest container ports in North America. In 2013, the port had 1,278 vessel calls and handled over 1.9 million TEUs.[15] Tacoma is the "Gateway to Alaska" and handles 80% of waterborne commerce from the lower 48 to Alaska. Tacoma's leading trade partners are China, Japan, Taiwan, Korea, Thailand, and Alaska. Top imports are vehicles, electronics, and machinery; the top exports are grain, meat, iron, and steel. The Port of Tacoma is diverse in space and facilities as well as its ability to handle containerized and non-containerized cargo from roll-on/roll-off (RO/RO) cargo, bulk, breakbulk, and heavy-lift/project cargoes.[16,17] The Port of Tacoma is also one of the west coast's Strategic Ports under the Ports for National Defense (PND).[18]

The Port of Everett, the third largest container port in the state, specializes in high and heavy cargoes,[19] such as manufacturing, constructing, mining, logs, wind energy, and aerospace. Boeing ships all oversized parts for the 747, 767, and 777 airplane programs through Everett. While the Port only had 175 vessel calls in 2013, it had a significant economic output due to the high value of the cargoes handled. Naval Station Everett and the USS Nimitz are homeported at the Port of Everett. The Port is also a hub for recreational boaters with the west coast's largest public marina.[20]

The Port of Olympia is on the Puget Sound's southern end and located in the urban center of Washington State's capitol city of Olympia in Thurston County. The port had 38 vessel calls in 2013 and specializes in breakbulk and project cargoes.[21] Weyerhaeuser is one of the Port's large specialized customers for the timber industry.[22] In additional to its marine facilities, the Port owns a recreational marine and boatyard facility, a regional airport, and commercial and industrial facilities.[23]

The Puget Sound Region is of considerable strategic importance to the continental United States. It is home to over 80,000 active duty military members from every branch of service. Joint-Base Lewis

[9] Washington Public Ports Association. (Retrieved August 2014). Port FAQS. http://washingtonports.org/washington-ports/about-our-ports/ports-faq/

[10] The port complex including Long Angeles and Long Beach is the first largest complex and Port Authority of New York and New Jersey is the second.

[11] The Port of Seattle also operates the Seattle-Tacoma International Airport.

[12] King County

[13] Port of Seattle. (2014). Seaport Statistics. http://www.portseattle.org/About/Publications/Statistics/Seaport/Pages/default.aspx

[14] Pierce County

[15] Port of Tacoma. (2014). Trade Statistics. http://portoftacoma.com/about/statistics

[16] Heavy-lift/project cargoes are large and awkward cargoes (*e.g.*, oil rigs) that may require custom handling.

[17] Port of Tacoma. (2014). Strategic Plan 2012-2022 Update.

[18] Military Surface Deployment and Distribution Commond Transportation Engineering Agency. (2010). Ports for National Defense.

[19] High and heavy refers to rolling cargoes which cannot be stowed in car carrier vessels due to their height and/or weight. Wallenius Wilhelmsen Logistics. (Accessed 3 September 2014). Glossary. http://www.2wglobal.com/support/glossary/#H

[20] Pacific Northwest Waterways Association. (2014). Washington's Puget Sound and Coastal Ports.

[21] Port of Olympia. (2014). "Seaport." http://www.portolympia.com/index.aspx?NID=9

[22] The Olympian. (October 12, 2011). "Weyerhaeuser lease has become key part of local economy."

[23] Port of Olympia. (2012). Port of Olympia 2013-2025: Strategic Plan Vision 2025.

McChord (JBLM) is the Army's west coast power projection platform and deployed over 90,000 troops in support of Operation Enduring Freedom, Operation Iraqi Freedom, and Operation New Dawn. JBLM is home to I Corps and the Air Force 62nd Air Wing (C-17s).[24]

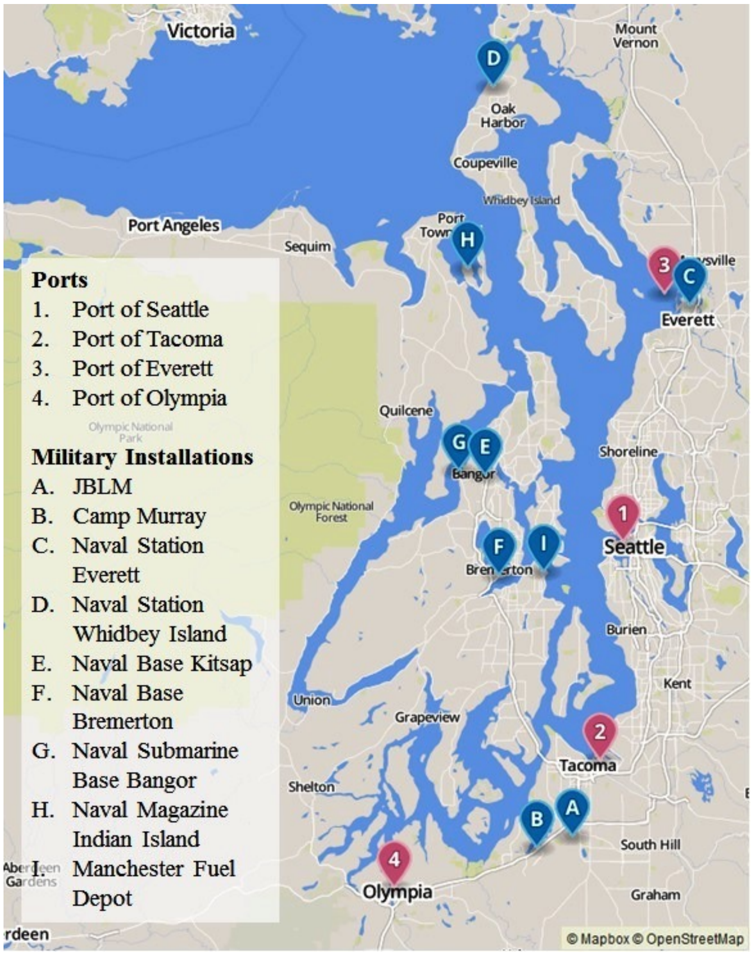

Figure 2.1: Geographical location of major ports and military installations.

The U.S. Navy has a large presence in Washington State. Naval Station Everett is home to the USS Nimitz. Naval Air Station Whidbey Island is home to all Navy tactical electronic attack aircraft flying the EA-6B Prowler and EA-18G Growler and provides search and rescue (SAR) for the area.[25] Naval Base Kitsap, the Navy's 3rd largest base in the U.S., includes Naval Station Bremerton and Naval Submarine Base, Bangor.[26] Naval Station Bremerton is home to the Puget Sound Naval Shipyards, the west coast dry dock for Nimitz class vessels, and the Navy's largest fuel depot. Naval Submarine Base, Bangor is home to the west coast Trident Submarines. Naval Magazine Indian Island (NMII), located in Jefferson County near Port Townsend, is the west coast's northern strategic ammunition port. It serves as the ordnance management center for fleet and shore stations in

[24] JBLM. (2014). http://www.lewis-mcchord.army.mil/

[25] CNIC. (2014). Welcome to Naval Air Station Whidbey Island. http://www.cnic.navy.mil/regions/cnrnw/installations/nas_whidbey_island.html

[26] CNIC. (2014). Welcome to Naval Base Kitsap. http://cnic.navy.mil/regions/cnrnw/installations/navbase_kitsap.html

the Pacific Northwest Region. It is the only active breakbulk and containerized ordnance transshipment port in support of the joint service of the Pacific command.[27] The Navy's Manchester Fuel Depot, across the Puget Sound from Seattle, provides bulk fuel and lubricant support to Navy activities and shore sites as well as to the USCG and visiting navy ships. It comprises 38 storage tanks with 60 million gallons of fuel and 11 miles of pipeline.[28]

The U.S. Coast Guard has a presence across the region, with its District 13 offices and Sector Puget Sound in Seattle and Coast Guard Stations in Seattle, Bellingham, Port Angeles, Neah Bay, and Quillayute River on the Pacific Coast. There is a USCG air station in Port Angeles.[29] The USCG, with the Canadian Coast Guard, provides CVTS for the Puget Sound.[30] Camp Murray serves as the Washington National Guard (WANG) headquarters and the state emergency operations center (EOC).[31] The Port of Tacoma and Naval Magazine Indian Island are strategic ports under the Ports of National Defense.[32]

Beyond the major ports and large military presence, the maritime community is complex, diverse, and large. Marine traffic is made up of tankers, freighters, excursion boats, cruise ships, recreation boats, tug and tow operations, ferries, military, law enforcement, search and rescue, and fire; each having a unique role in the maritime community. The community expands off the water to include multiple organizations. Governmental organizations at every level that play both direct and indirect roles in the community include:

- U.S. Customs and Border Patrol (CBP)
- Department of Transportation (DOT)
- DOT Marine Administration (MARAD) Department
- U.S. Army Corps of Engineers (USACE)
- Department of Ecology (DOE)
- U.S. Fish and Wildlife
- Occupational Safety and Health Administration (OSHA)
- Federal Emergency Management Agency (FEMA)
- Legislative bodies from the city to federal level
- Tribal Governments and agencies

It is important to note that when talking about the maritime community it expands beyond just organizations that are directly focused on a marine environment. There are private companies and

[27] Commander, Navy Installations Command. (Retrieved 3 September 2014). "Naval Magazine Indian Island Mission and Vision." http://www.cnic.navy.mil/regions/cnrnw/installations/naval_magazine_indian _island/about/mission_and_vision.html

[28] Global Security. (2014). Manchester Navy Fuel Depot. http://www.globalsecurity.org/military/facility/manchester.htm

[29] USCG. (2014). Units by State. http://www.uscg.mil/d13/units/state.asp

[30] United States Coast Guard. (2013). The 2013 Vessel Traffic Service User Manual.

[31] Washington State National Guard Joint Forces. (2014). The New Emergency Operations Center. http://washingtonguard.org/news/archive/fo-eoc.shtml

[32] Military Surface Deployment and Distribution Commond Transportation Engineering Agency. (2010). Ports for National Defense.

volunteer organizations both with a land-based and marine-based economic focus that are part of the maritime community such as trucking companies, rail companies, labor unions (*e.g.*, International Longshore and Warehouse Union), pilots, Marine Exchange, Pacific NorthWest Economic Region (PNWER), and the USCG Auxiliary. There are also those organizations that provide services such as law enforcement, fire, search and rescue, fusion center, emergency operations centers (EOCs), and educational institutions. Because of Washington's border and shared waterways with Canada, Canadian FSLTIPP entities are also stakeholders in the Puget Sound. Many of the trade partners and private corporations in the Pacific Northwest are international.

The Pacific Northwest, and specifically the Puget Sound area, was chosen for the MOISA project due to many factors. The area has a robust and mature maritime community. The stakeholders cover all facets of commercial, private, federal, and international business. The University of Washington has participated in several previous activities within the community and has a Memorandum of Agreement (MOA) with the very active Area Maritime Security Committee to be its research arm. Geographically the area is large and is unique with its strong coordination with Canada through the CVTS.

Over the last decade, the University of Washington (UW) has developed a close working relationship with the Puget Sound safety and security community. In 2004, as part of a DHS sponsored consortium under the newly chartered National Visualization and Analytics Center at the Pacific Northwest National Laboratory, the UW established the Pacific Rim Visualization and Analytics Center (PARVAC). In January 2008, Professor Mark Haselkorn, one of the principal investigators for MOISA, became the Director of PARVAC and led a multi-year effort to enhance information sharing capabilities in the region.

In February 2009, the Area Maritime Security Committee (AMSC) and the UW signed a MOA that established,

> terms and procedures by which the AMSC and the PARVAC, through the University of Washington, will establish a leadership structure and facilitating mechanism for cooperative research on safety and security issues to make more efficient use of resources available within the geographic boundaries of the Puget Sound Federal Maritime Security Coordinator's jurisdiction.[33]

Under this umbrella, UW researchers and students partnered on a number of projects to enhance regional information sharing capabilities, including one research effort to demonstrate enhanced situational awareness and communication that went operational

[33] Memorandum of Agreement Between the Seattle Area Maritime Security Committee and the University of Washington's Pacific Rim Visualization and Analytics Center Regarding Cooperative Research-Related Activities, signed by U.S. Coast Guard Captain of the Port on February 19, 2009 and by University of Washington Director of the Office of Sponsored Programs, February 28, 2009.

when a 2010 DNDO on-water exercise lost its covered communications.[34] Perhaps more importantly, UW researchers have become trusted and active members in this vital maritime community.

As we write, PARVAC has been replaced with a new Center for Collaborative Systems for Security, Safety, and Regional Resilience (CoSSaR) that is focused on broad participation of regional stakeholders. USCG Sector Puget Sound and CoSSaR are working together to update the MOA and take advantage of new knowledge, capabilities, and opportunities provided through CoSSaR and the ongoing MOISA project.

[34] Reported in Benson, A.L., Biggers, K., Wall, J., and Haselkorn, M.P. (2010) "Adaptive Development of a Common Operating Environment for Crisis Response Management." In *Proceedings of the 2010 International Conference on Information Systems for Crisis Response and Management*

3 Literature Review and Known Issues

AFTER 9/11, the United States government moved swiftly to increase its border security and increase coordinated action. The Department of Homeland Security (DHS) was created in 2002, and the U.S. Congress introduced nine new pieces[1] of legislation relating to maritime security between September 11, 2001 and May 21, 2002. Commercial shipping was an area of focus due to its large impact on the American economy. Maritime commerce relies on the access of people and cargo to American shores, and therefore, both the waterfront and land-side infrastructure are open to attack. Even more impactful than the immediate commercial loss are the damage to the transportation network and the economic consequences of delaying commerce. The Congressional Budget Office estimates that a closure of the Ports of Long Beach and Los Angeles would cost the U.S. economy a maximum of $190 million per day.[2] Efforts have and continue to be made to increase maritime domain awareness (MDA) and increase transparency among international, federal, state, local, tribal, private, and public maritime stakeholders.

Transparency of information in the maritime domain has been a source of controversy. As we found in our review of the PSSSC's ISE, economic competition can create legitimate reasons for secrecy in the maritime domain that are not connected to malicious intent. One instance which has been debated in post-9/11 maritime security literature is that of vessel ownership anonymity. The lack of transparency of ownership was instituted in order to encourage investment in an inherently risky business. Vessel owners have limited liability, but limited liability is not absolute, and therefore, anonymity was introduced to protect owners in the case of a casualty.[3] A second instance of legitimate secrecy is in the commercial fishing industry. Fishermen will either refrain from disclosing information or provide misinformation to other fishermen in order to obtain more of the limited common resource.[4] Inter- and intra-port competition are also

[1] The Port and Maritime Security Act of 2001; the Port Threat and Security Act; the United States Security Act of 2001; the Port Security and Terrorism Prevention Act; the Enhanced Border Security and Visa Entry Reform Act of 2002; the Maritime Transportation Antiterrorism Act of 2002; the Ship, Seafarer, and Container Security Act; the Port Terrorism Prevention Act of 2002; and the Reducing Crime and Terrorism at America's Seaports Act of 2002.

[2] In 2014 dollars. Congressional Budget Office. (2006). The Economic Cost of Disruptions in Container Shipments.

[3] Fox, J.B. (2005). Vessel Ownership and Terrorism: Requiring Disclosure of Beneficial Ownership in Not the Answer. *Loyola Maritime Law Journal (4).*

[4] Palmer, C.T. (1990) Telling the Truth (Up to a Point): Radio Communication Among Maine Lobstermen. *Human Organization*, Vol. 49, No.2

drivers of secrecy. Terminals operating at the same port provide the same geographic advantages (*e.g.*, ocean voyage distance, hinterland connections) to customers and must compete on the basis of terminal operations.[5] Terminals have an incentive to keep their operations secret to avoid their intra-port competitors from poaching their customers.

To achieve effective information sharing, mechanisms need to be in place to encourage maritime industry participants to overcome their predisposition to privacy. One important step in supporting information sharing is reciprocity. The Maritime Information Sharing Taskforce found that Puget Sound participants perceived a lack of reciprocity with federal partners and viewed information sharing as a one-way interaction from themselves to the Federal Government.[6]

One forum for information sharing that is praised by the community is the Puget Sound Area Maritime Security Committee (AMSC). The Maritime Transportation Security Act of 2002 established AMSCs in all major port sectors. Led by the Captain of the Port, the AMSC is responsible for convening federal and nonfederal stakeholders to create area security plans. The Puget Sound AMSC is a highly successful structure for reciprocal information sharing based on relationships and trust building.

Another formal information sharing structure is the interagency operations centers (IOCs) which were mandated by the Security and Accountability for Every Port (SAFE Port) Act of 2006. The three main capabilities of an IOC are (1) integrated vessel targeting, (2) interagency operational planning, and (3) operations monitoring. IOC information is collected, organized, and disseminated using the USCG WatchKeeper system. Ninety-six hours prior to a vessel arriving at a U.S. port of entry, the IOC integrated vessel targeting team evaluates the arriving crew, vessel, and cargo. The vessel arrival information along with state-of-the-port information is accessible to the USCG, CBP, state and local law enforcement, and other port partners.[7]

One of the main goals of reciprocal information sharing is situation awareness, which can be delivered through a common operating picture (COP). COPs are frequently displayed in a GIS viewer. In the maritime domain, WatchKeeper functions as the U.S. Coast Guard's GIS viewer and displays data collected and maintained in other government-owned systems.[8] WatchKeeper, however, was not designed to meet non-government port partners' needs and is seldom used outside of the USCG.[9]

A COP relies on information sharing and integration. One obstacle to developing a useful COP is the difficulty in sharing and integrating information from resources that are not at the

[5] Notteboom, T. (2008). The Relationship Between Seaports and the Intermodal Hinterland in Light of Global Supply Chains: European Challenges. Joint Transport Research Centre Discussion Paper No. 2008-10.

[6] Salem, A., Walsh, W., & Englehorn, L. Maritime Information Sharing Taskforce. Naval Postgraduate School (2009). Industry and Public Sector Cooperation for Information Sharing: Ports of the Puget Sound.

[7] Government Accountability Office. (2012). Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers. (GAO Publication No. 12-202). Washington, D.C.: U.S. Government Printing Office.

[8] CAPT Wilbur, R.S. and Cantor, J.R. (2013). Privacy Impact Assessment for the Interagency Operations Center (IOC) WatchKeeper DHS/USCG/PIA.

[9] Only 18% of the port partners accessed WatchKeeper and only 3% accessed it more than five times in September 2011. Government Accountability Office. (2013). Coast Guard: Observations on Progress Made and Challenges Faced in Developing and Implementing a Common Operational Picture. (GAO Publication No. 13-784T

same classification level and can, therefore, neither be directly nor easily integrated.[10] The issue of classification affects more than COP technology. In a 2005 GAO report, for example, a Washington State Ferries official cited lack of a security clearance as the reason he was unable to carry out his security duties. Specific information was known by the U.S. Attorney's Office and the USCG that would have aided the WSF official in preventing illegal activity.[11]

The National Network of Fusion Centers, mandated by the 9/11 Commission Act of 2007,[12] receives both unclassified and classified data. In 2013, 65 centers had access to the Homeland Secure Data Network which is a SECRET network and 45 of those centers had access to FBINet. Fusion Centers receive data from federal agencies, analyze the data in the local context, and disseminate relevant data to local partners. Additionally, they gather and analyze local data and pass it on to federal agencies.[13] The Washington State Fusion Center (WSFC) is one third of the Statewide Integrated Intelligence System (SIIS) which was created in 2002. The WSFC uses the Situational Awareness and Watch Center (SAWC) to share information products, such as briefings, bulletins, assessments, and requests for information. The Puget Sound Regional Catastrophic Disaster Coordination Plan calls for WSFC to play an important regional role in information integration.[14] Our review of the PSSSC's ISE added considerable insight into the issues of classification and the role of the Fusion Center.

Other federal integration efforts are less focused on day-to-day information sharing and more focused on larger initial sharing efforts to decrease risk and prioritize federal efforts. In 2001, the U.S. Customs and Border Protection Agency (CBP) established the Commercial Operations Advisory Committee (COAC), which initially consisted of 50 international trade industry experts. COAC gave CBP an expanded view of security in the context of international trade. A highly respected trade professional and member of the COAC until 2004, Michael D. Laden,[15] stated that, prior to COAC,

> CBP did not know how an international or multinational supply chain really worked. What data was available? Who are the stakeholders? What are the mechanics and touch points? Prior to 9/11, most CBP inspectors and personnel only knew that a consignment had presented itself at a port of entry into the U.S.; and now their job in determining admissibility and collecting duties began. They knew very little about what had happened upstream with the consignment before the cargo arrived.[16]

Once aware of their incomplete knowledge of the supply chain, CBP responded by launching the strictly voluntary Customs-Trade Partnership against Terrorism (C-TPAT) in 2001. The idea behind

[10] Government Accountability Office. (2013). Coast Guard: Observations on Progress Made and Challenges Faced in Developing and Implementing a Common Operational Picture. (GAO Publication No. 13-784T). Washington, D.C.: U.S. Government Printing Office.

[11] Government Accountability Office. (2005). Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. (GAO Publication No. 05-394). Washington, D.C.: U.S. Government Printing Office.

[12] Implementing Recommendations of the 9/11 Commission Act of 2007, H.R. 1, 100th Cong. §511 (2007).

[13] Program Manager, Information Sharing Environment. (2013). Information Sharing Environment: Annual Report to the Congress.

[14] In Puget Sound Regional Catastrophic Disaster Coordination Plan. (2012). Fusion Center Integration Report.

[15] Michael Laden is a member of the Customs Trade Support Network which works with CBP to build the Automated Commercial Environment (ACE) system. He is also a member of the World Customs Organization (WCO) Task Force on Security and Facilitation.

[16] Laden, M. (2007).The Genesis of the U.S. C-TPAT Program: Lessons Learned and Earned by the Government and Trade. *World Customs Journal*, Volume 1, No.2., pg. 77.

C-TPAT is that trade members provide CBP with information about the security of their supply chain and are, therefore, "known," requiring fewer inspections. Nonmembers are "unknown," and require more attention by CBP.[17]

As stated in a 2008 study, the annual cost to importers participating in the C-TPAT program was $30,000. However, the benefits of C-TPAT to these participants was not being realized uniformly — only 33% reported that the benefits outwieghed the costs.[18] CBP also provides importers an incentive to correct errors in importation paperwork through the Importer Self-Assessment (ISA) program. If the importer notifies CBP of the error prior to CBP becoming aware of it, the importer's penalty will be reduced.[19] Many trade professionals view these programs as a way to shift some of the burden of ensuring security of the supply chain onto the trade industry and not as a mutually beneficial information sharing environment.[20] As one of MOISA's conclusions is the need to refine federal and regional partnerships, C-TPAT and ISA provide interesting background.

In addition to programs like C-TPAT and ISA, other programs affect cargo-related information sharing and associated safety and security. CBP instituted the 24-hour advance vessel manifest rule in 2003. The rule's goal is to identify high risk containers before they arrive at a U.S. port of entry. The cargo manifest is the primary input into the Automated Targeting System (ATS),[21] and no other information is mandatory for the container's risk assignment.[22] The International Maritime Organization (IMO) found, however, in a study of seven participating countries[23] that 32% of 25,284 inspected containers had cargo misdeclarations.[24] Dangerous cargo may be misdeclared in order for the shipper to avoid paying higher transport costs, but the misdeclaration of dangerous cargo has been blamed for marine casualties on multiple occasions. Dangerous cargo, when misdeclared, may be improperly stowed below deck and can cause catastrophic damage to the vessel upon fire or explosion.[25] To reduce cargo-related casualties, five of the main ocean carriers [26], jointly formed the Cargo Incident Notification System and Organization (CINS) in 2010. CINS collects data on cargo incidents and has attributed 27% of incidents between June 2011 and September 2013 to misdeclarations.[27]

The literature underscores that the security of the maritime transportation system cannot be maintained solely by point of entry facility security (*e.g.*, guards, fences, inspectors). Security needs to be a fundamental element of day-to-day operations, with ongoing work-related information sharing a key element in the process. Given the diverse and interconnected nature of maritime operations, it is critical to "ensure that security gaps are not created where

[17] Laden, M. (2007).

[18] Peterson, J. and Treat, A. (2008). The Post-9/11 Global Framework for Cargo Security. *U.S. International Trade Commission Journal of International Commerce and Economics.*

[19] Customs and Border Protection. (2002). Importer Self-Assessment Program: General Notice. (4820-02-P).

[20] Giermanski, J.R. (2013). Global supply Chain Security.

[21] DHS/CBP/PIA-006(c)

[22] Government Accountability Office. (2004). Homeland Security: Preliminary Observations of Efforts to Target Security Inspections of Cargo Containers. (GAO Publication No. 04-325T). Washington, D.C.: U.S. Government Printing Office.

[23] Belgium, Canada, Chile, Italy, the Republic of Korea, Sweden, and the United States.

[24] International Maritime Organization. (2006). Sub-Committee on Dangerous Goods, Solid Cargoes, and Containers. Report to the Maritime Safety Committee. (DSC 11/19). 11th Session. Agenda Item 19.

[25] Foster, C. (2007). Misdeclared or Undeclared Dangerous Goods Cargoes. Swedish Club Letter.

[26] CMA-CGM, Evergreen, Hapag-Lloyd, Maersk Line, and Mediterranean Shipping Company.

[27] Velde. D.V. (2014).The Cargo Incident Notification System and Organisation. Standard Cargo Special Edition: Misdeclared Cargo.

individual modes of transportation interconnect and where public and private sector jurisdictions and responsibilities begin and end."[28] The literature's attention to interdependency and incorporating user needs forms the foundation for MOISA1. Maritime operations are a large, diverse, and interconnected system where safety and security depend upon the organization of many individual operators and entities into a community that supports effective and efficient information sharing and coordination. The literature reports on many federally-led initiatives to cultivate information sharing among these entities — initiatives that have achieved uneven results. There is a connection between these uneven results and then MOISA1 story of a complex regional safety and security community that achieves results on a day-to-day basis largely through self-organization and trust-based relationships.

[28] Committee for a Study of the Federal Role in the Marine Transportation System. (2004). Special Report 279, The Marine Transportation System and the Federal Role: Measuring Performance, Targeting Improvement. Transportation Research Board, Washington, D.C. pg. 36.

4 Project Overview

The maritime domain is defined by the U.S. Maritime Security Policy[1] as

> All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.

The maritime community includes any organization or individual with an active role in this vast maritime domain, and therefore can be extremely difficult to demarcate. For example, during MOISA1 when the Department of Ecology called for a tightening of dumping restrictions in the Puget Sound, it potentially affected vessel operations and became an issue of concern for the Harbor Safety Committee. Does that make the Department of Ecology a member of the maritime community?

While identifying and understanding the regional maritime safety and security community is a difficult task, it is the only way to begin a project like MOISA. This is primarily because the goal of MOISA is not to investigate *systems for the community* but to investigate the *community as a system*. From this perspective, the members of the maritime community are the key components of a complex socio-technical service system that provides ongoing safety and security to the region. Therefore, MOISA began with a broad study of information sharing among representatives of the regional maritime safety and security community.

This shift from a technology-centric approach to a human- and community-centric approach is as fundamental and impactful to MOISA as the shift from incident-focused security to day-to-day operations-focused security (discussed in Section 1). Viewing the day-to-day operations of the maritime community as the primary elements of the regional maritime safety and security system puts people's missions, along with their work processes and information sharing in support of mission accomplishment, at the center of our system analysis.

[1] National Security Presidential Directive-41/Homeland Security Presidential Directive-13.

We began by studying people and communities of work, not to understand them as users of systems, but to engage with them and help them articulate the nature of the system of interest, of which they are the key component.

We identify and align investments in regional safety and security, not by asking questions such as "Will these radios communicate with each other?" or "Will these common operating picture (COP) technologies share this sensor data?" but rather, "Will this investment be adopted and owned by community members, and will it enable them to better work together and share information in support of their missions?" An important benefit of this community-centered approach is the opportunity to build on the researchers' long-standing relationship with the maritime community and to build new partnerships, and gain trust for ongoing collaborative MOISA efforts.

MOISA Sample

FSLTIPP Category	Organizations
Federal	12
International	4
State	6
Local	17
Tribal	3
Private	5
Overlapping	5

Table 4.1: The FSLTIPP category of the organizations represented in the Phase 1 sample of the community.

The initial set of community representatives chosen to participate in this study was guided by the FSLTIPP schema (see Table 4.1). Year one study participants consisted of 77 individuals representing 52 organizations (see Section 5 for more detail).

We conducted semi-structured interviews with this population to gather information on several topics, including:

- Willingness and authority to share information
- Regional and multi-agency organizational structures for information sharing
- Policy affecting operational information sharing
- Business processes in place to enable situational awareness
- Systems in use to enable situational awareness
- Difficulties and unmet information needs

We supplemented the interviews with a literature review that included government reports, academic literature, and primary resource documents collected from the field, such as meeting rosters and agendas. We also immersed ourselves into the community, attending and participating in local and regional events, conferences, and presentations and conducting informal interviews with individuals outside the Phase 1 sample. The information collected from the formal interviews and the numerous other interactions with the community form the basis of the analysis described in Section 5. The results of the analysis can serve to inform information sharing requirements and to guide future investments and key decisions associated with designing and fielding policy and technical solutions.

The Phase 1 analysis spans the entire FSLTIPP of the maritime community with a goal of capturing common themes among the stakeholders. MOISA also includes a Phase 3 analysis that focuses on one major activity in the maritime domain — container terminal cargo operations. This choice of use-case was identified in Phase 2. Phase 3 demonstrates a human-centered evidence-based methodology for putting work and information requirements at the center of future investments to improve the system. It does this by modeling, in detail, the activity's flow of work and information in order to identify information exchange requirements.

While Phase 1 provides critical understanding of the overall system and its environment, it does not contain enough detail to guide how a specific intervention should be designed and implemented nor does it specifically anticipate unintended effects on current workflows. This level of detail is contained in Phase 3; our model of container terminal operations can both identify which specific areas of work will be affected by a given intervention and provide an information architecture that can be used to assure that information resources are organized effectively. In summary, Phase 1 identifies aspects of information sharing that might benefit from intervention, Phase 3 supplies a tool to analyze alternative interventions, and then Phase 1 contributes to evaluating whether the design of the interventions are acceptable to the community. Issues such as dependence on appropriate clearance levels and personal relationships that are identified as difficulties in Phase 1, but not captured in the Phase 3 model, will shape the set of potential interventions.

This report is organized by the three interdependent phases (see Figure 4.1) used to conduct the research. An analysis focused on IT system particulars, such as identity management and data standards, is included as an adjunct to Phase 1 (Section 6).

4.1 *Phase 1: The Community and its Information Sharing Environment*

The objective of Phase 1 is to produce a broad understanding of the maritime security interagency information environment and how organizations interact during day-to-day operations, with focus on information dependencies. We collected qualitative data from interviews with stakeholders across the FSLTIPP, and we recorded field observations of meetings, exercises, and workshops. Using this raw data, we conducted a qualitative analysis to identify key themes common across the community.

4.2 Phase 2: Interagency Dependencies and Use-Cases

The objective of Phase 2 is to explore interagency information dependencies, identify common use-cases within the community, and develop criteria to select a single use-case for an exploratory analysis in Phase 3. Candidate scenarios were derived from an analysis of Phase 1 data. We scored these candidate use-cases based on criteria, such as degree of interdependence required, in order to down-select to a single use-case and identify the boundaries of the Phase 3 model.

4.3 Phase 3: Modeling Containerized Cargo Operations Use-Case

The objective of Phase 3 is to demonstrate the effectiveness of a model-based systems engineering approach for understanding the way current information resources constrain workflows and to support the design of community-driven collaboration. To achieve this aim, we conducted an in-depth analysis of the use-case selected in Phase 2 — container terminal cargo operations. We then modeled the flow of tasks that drive scenarios within this use-case and analyzed the use of security information that supports cargo operations, as well as implications for the design and implementation of information and communication interventions using examples from current federal initiatives.

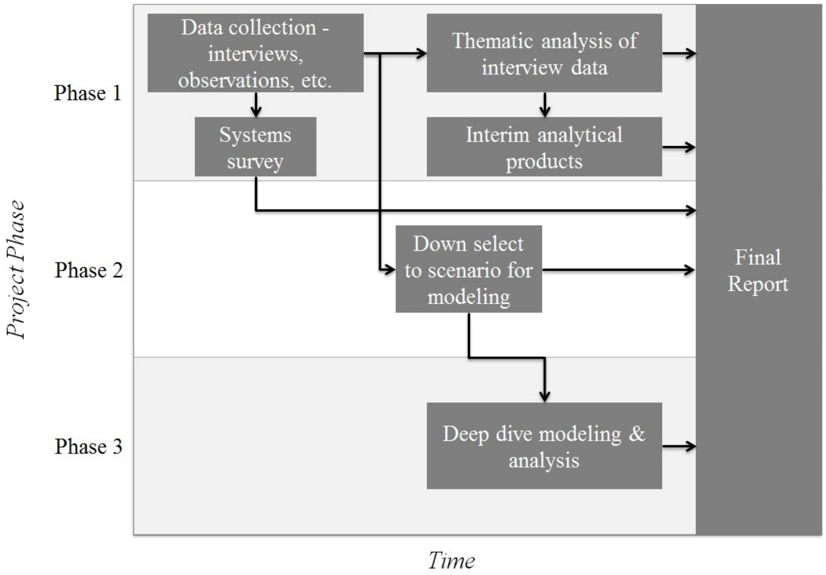
Data collection - interviews, observations, etc.
Thematic analysis of interview data
Phase 1
Systems survey
Interim analytical products
Project Phase
Phase 2
Down select to scenario for modeling
Final Report
Phase 3
Deep dive modeling & analysis
Time

Figure 4.1: How the three phases of the project research relate to each other.

5 Phase 1: The Community and its Information Sharing Environment

5.1 *Summary*

As has been discussed above, the primary aim of MOISA1 was to investigate the Puget Sound maritime "community as a system" and produce a broad understanding of the community's information sharing environment (ISE). Phase 1 was critical to this aim and represented the majority of the project effort. In Phase 1, we conducted a qualitative, thematic analysis of interview and observational data. In this section, we restate the Phase 1 objectives and present the Phase 1 methodology, analysis, results, and findings.

5.2 *Objectives*

The objectives of Phase 1 were to:

- Interact with a broad cross-section of diverse stakeholders within the Puget Sound maritime community.
- Understand day-to-day operations in support of safety and security.
- Discover security-related information sharing practices and perspectives from multiple stakeholders in the community.
- Learn how community members think about their role in maritime security.
- Conduct an evidence-based qualitative analysis of information sharing practices, successes, and difficulties.
- Learn how communication and information technologies fit into the information sharing practices of the community.

5.3 Methodology

During Phase 1 of MOISA, we observed and interviewed participants in the Puget Sound maritime community to discover and characterize information sharing activities related to safety and security. To develop a contextual understanding of the community and its challenges/successes, we participated in and observed numerous exercises, attended many community meetings, conducted formal face-to-face interviews with dozens of community members, and reviewed published literature and related resources. We collected and systematically examined a data set of interview notes, meeting observation notes, and literature sources to guide the analysis that follows.

5.3.1 Population

Interviewees for the formal, face-to-face interviews were selected to represent the geographical (Figure 5.1), cultural, and organizational diversity of the Puget Sound maritime community. To identify candidates for interviews, we worked with an Interagency Operations Center (IOC) liaison based at the U.S. Coast Guard, Sector Puget Sound to develop a list of desirable organizations to interview. We maintained and monitored this master list while scheduling interviews. In a selection process known as snowball sampling,[1] we periodically expanded our list of desired interviewees by using information gathered from initial interviews to refine our definition of who should be consulted. This process expanded an initial list of 32 organizations targeted for interviews to 52 organizations. Ultimately, 58 formal interviews were conducted with 77 interviewees representing the 52 organizations. Some organizations (*e.g.*, USCG) were represented by multiple interviewees, which enriched the overall data set. Most organizations, however, were represented by a single interviewee.

To ensure that we captured a diverse set of perspectives from across the community, we were initially guided by the FSLTIPP schema (Federal, State, Local, Tribal, International, Public, Private), seeking to include more than one entity from each of those categories. While the FSLTIPP designation proved to be a helpful heuristic for gaining multiple perspectives, five organizations could arguably be placed into multiple categories. For example, one organization identified as playing a key role in maritime information sharing is the Pacific Northwest Economic Region (PNWER). It describes itself as a

[1] "Snowball sampling may be defined as a technique for gathering research subjects through the identification of an initial subject who is used to provide the names of other actors. These actors may themselves open possibilities for an expanding web of contact and inquiry. The strategy has been utilized primarily as a response to overcome the problems associated with understanding and sampling concealed populations." Encyclopedia of Social Science Research Methods. (2004). 'Snowball Sampling.' SAGE Publications, Inc. Retrieved from http://srmo.sagepub.com/view/the-sage-encyclopedia-of-social-science-research-methods/n931.xml

"statutory public/private nonprofit"[2] and has a presence both in the U.S. and Canada. Organizations that fall into more than one category are represented in Table 5.1 as "overlapping." See Appendix C for the full list of organizations that were formally interviewed in Phase 1.

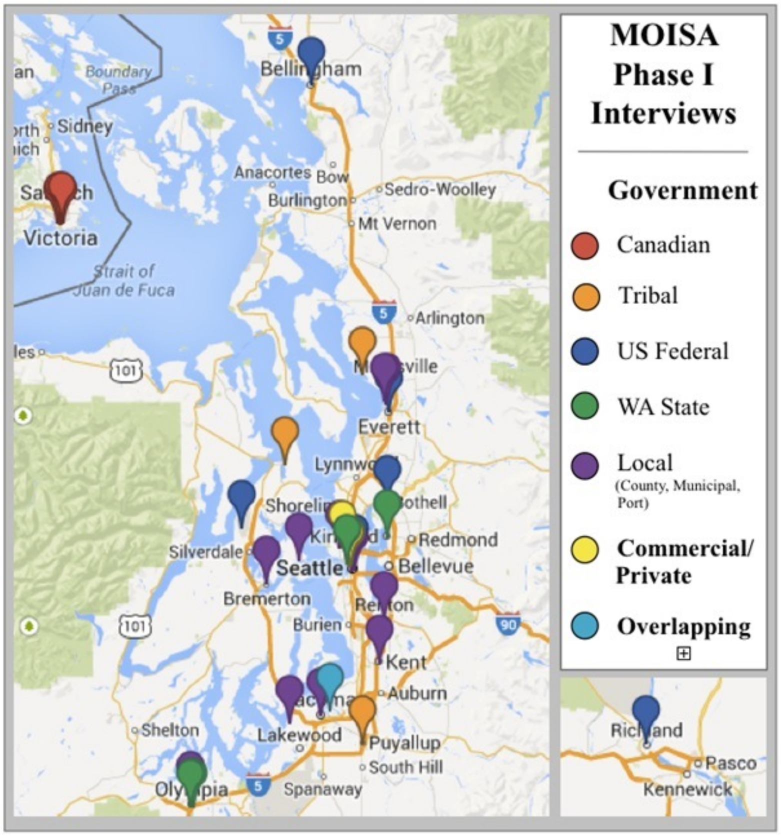

Figure 5.1: The location of formal interviews colored according to their FSLTIPP designation.

In addition to organizational diversity, the individuals interviewed tended to represent different perspectives within their organizations with over 50 unique job titles among them. Our approach was to talk to people in each organization who engage in interagency activities with an emphasis on those responsible for safety and security who were willing to schedule time with our interview teams. Our ability to interview people filling different types of roles in these organizations (*e.g.*, supervisors, officers, executives, information specialists) yielded a larger interview set than we might have achieved otherwise. Interviewees represented a range of tactical, strategic, and operational positions. In this way, we realized a much richer, more diverse data set than we would have had we only interviewed individuals in a specific role, such as the those at the top of each organization.

[2] PNWER. (2014). "About Us." http://wwww.pnwer.org/about-us.html

5.3.2 *Data Collection*

The primary method of data collection in Phase 1 was semi-structured formal interviews that probed the information sharing practices, dependencies, and needs of community members. To distinguish the 58 interview events conducted with 77 interviewees from other data collection activities that occurred in Phase 1, we refer to those interviews that followed the Phase 1 interview protocol as "formal interviews." These took place between November 2013 and June 2014. Each interview was led by an experienced qualitative researcher from the University of Washington's Department of Human Centered Design & Engineering. Interview teams typically consisted of one interviewer and one note-taker. Interviews were conducted with between one to five interviewees and typically lasted one hour. Most occurred at the interviewee's place of work.

FSLTIPP Category	Organizations	Interviewees
Federal	12	25
International	4	8
State	6	9
Local	17	19
Tribal	3	4
Private	5	6
Overlapping	5	6

Table 5.1: The FSLTIPP designation of interviewees who were formally interviewed.

The interview protocol for the formal interviews was developed through an iterative process. A pilot protocol was used with six interviewees in November and December of 2013. After these initial interviews were completed, the entire team met to refine the interview protocol and establish a final protocol that would be used in all subsequent interviews (see Appendix D for the full protocol). This protocol was used in 52 interviews, from January 2014 until June 2014. The pilot protocol was structured and comprehensive, and the data was retained for the final dataset. However, given the diversity of organizations and job roles represented, it was found to be somewhat restrictive and lengthy.[3] The final protocol employed a semi-structured format to allow for shorter interviews with broader data collection that provided greater latitude for the interviewee. Interview leaders used discretion to determine which topics in the protocol to emphasize with particular interviewees.

The Phase 1 interview protocol combined open-ended discussion topics that gave room for interviewees to self-describe their information sharing practices with closed questions on specific aspects of information sharing. Interviewees were asked to describe their job role, work context, and how much of their mission concerned security. We asked interviewees about their information dependencies (*i.e.*, who relies on the interviewee for information, and who they rely on for information); the trigger and purpose behind instances of information sharing; the process they use to share information; and what information resources they employed in the course of their work. Interviewees were asked to describe information gaps or challenges that they experienced when obtaining or sharing information. In addition, we asked interviewees about specific

[3] "Respondent fatigue is a well-documented phenomenon that occurs when survey participants become tired of the survey task and the quality of the data they provide begins to deteriorate." Encyclopedia of Survey Research Methods. (2008). 'Respondent Fatigue.' Sage Publications, Inc. Retrieved from http://srmo.sagepub.com/view/encyclopedia-of-survey-research-methods/n480.xml

aspects of information sharing: their perceptions on the impact of regulation, policy, agreements and Memoranda of Understanding (MOUs) on information sharing; the influence of organizational culture and values of interagency information sharing; and the use of social media in their work. Finally, a series of structured questions concerning information sharing in relation to radiological/nuclear detection were asked. Responses to information sharing pertaining to radiological/nuclear detection were shared with the Domestic Nuclear Detection Office (DNDO) and are reported separately in Appendix G.

In addition to conducting formal semi-structured interviews, MOISA team members attended and participated in over 30 community events during Phase 1 including meetings, exercises, workshops, local and regional events, conferences, and presentations. When formal interviews were not possible, such as when a potential interview only had time to answer a few questions, we conducted informal interviews. While all these interactions provide background for and confirmation of our analysis, only a portion (11 events) of those that were documented are included in the dataset for the Phase 1 data analysis.

5.3.3 *Analysis*

Phase 1 data consists of 69 field notes (58 formal semi-structured interviews and 11 field observations of community activities). Of these, 66 field notes were documented by note-takers and 3 were audio-recorded and transcribed.

In order to produce a broad understanding of the maritime safety and security interagency information environment and how organizations interact during day-to-day operations, we conducted a thematic analysis of the Phase 1 data.

Data were imported into a qualitative data analysis software tool.[4] Within the tool, we identified related content across the data set and labeled the related content with a qualitative code.[5] For most of the codes applied, researchers coded the data independently and then conducted debriefing sessions to review discrepancies and achieve consensus on the final code applications. This assured consistency in how codes were applied.

Related content was summarized into memos that were discussed by the full team.[6] This process supported both the analysis of themes of interest that the team had identified prior to going into the field (*e. g.*, the role of MOUs in information sharing), as well as unanticipated themes that emerged during the interviews (*e.g.*, the role of trust

[4] Dedoose. http://www.dedoose.com/

[5] Saldaña, J. (2012). The Coding Manual for Qualitative Researchers (No 14). Sage Publications, Inc.

[6] Miles, M.B., Huberman, A.M., and Saldaña, J. (2013). Qualitative Data Analysis: A Methods Sourcebook. Sage Publications, Inc.

in information sharing). Field notes were first coded for the topics in the interview protocol. Then additional sub-themes within each component of the protocol were coded. Emergent themes identified by reading the text — such as collaboration, trust, resource alignment, and turnover of personnel — were also coded. In all, 7 researchers applied more than 180 codes and descriptors 7,600 times to nearly 2000 excerpts of text.

Given the mandate of the project, much of the thematic analysis reported here focuses on the 795 excerpts in the data set that represent instances of information sharing as described by interviewees. These comprise descriptions of information sharing offered by interviewees in the course of answering questions about the information sharing they engage in during their day-to-day work.

Additional codes emerged from the thematic analysis that were not central to our primary theme of information sharing. Although these additional codes were applied to the data, they have yet to be fully analyzed and thus an analysis of these codes is not reported here. For a list of codes, see Appendix E.

5.3.4 *Day-to-Day Versus Incident-Focused Information Sharing*

We found during our interview process that it can be difficult to distinguish day-to-day operations from incident-focused information sharing. As mentioned earlier, during our interviews we focused the conversations on what interviewees do every day, but interviewees still frequently framed discussions of their information sharing in relation to incidents.

One reason interviewees may have tended to focus on incidents is that, to them, day-to-day operations are less compelling and visible than incident-focused operations. When day-to-day operations are successfully executed, nothing happens — there is no incident. Rarely do we have visibility into the number of incidents, crises, and disasters that are avoided on a day-to-day basis as the result of the successful collaboration of the numerous stakeholders in our community. In contrast, incidents are very visible and often highly publicized. In addition, we specifically asked interviewees who their information-sharing partners are, and because, in some cases, they only work with specific partners in the event of an incident, listing information sharing partners naturally caused some interviewees to recall incidents and the associated information sharing partnerships.

Research in psychology points to another reason why distinguishing day-to-day information sharing from incident-based information sharing may have proved challenging for interviewees: Day-to-day operations are often procedural and tacit, and particularly for experts like the interviewees in our sample, recalling procedural knowledge is difficult. This phenomenon is called "expertise induced amnesia." However, human recall is improved with more context. Focusing on an incident enables people to talk about procedural memory in relation to an explicit event, as the connection of procedural memory to an explicit event makes it easier for people to recall what they do and how they do it.[7] (This principle is being applied in Phase 3 of MOISA1 when we use the context of workflow to improve memory of where, what, and how information is used.)

Throughout our analysis, we do not attempt to distinguish what operations are day-to-day versus incident-focused, but rather we rely on the interviewees self-reported understanding of what constitutes their day-to-day activities — whether they discussed these in the context of incidents or not.

5.4 *Outline of Results*

The results of our analysis are important themes that shape the community ISE. These themes are presented in three parts: (1) what we learned about the community, (2) what we learned about the information sharing environment, and (3) the alignment of information technology with mission and workflow. These themes are organized under the three sections as follows:

5.5 What we learned about the community

- *5.5.1* Diversity
- *5.5.2* Community of doers

5.6 What we learned about the information sharing environment

- *5.6.1* Competition
- *5.6.2* Trust
- *5.6.3* Clearance levels
- *5.6.4* The relationship between day-to-day operations and incidents
- *5.6.5* Formal versus informal information sharing practices
- *5.6.6* Information sharing with the public
- *5.6.7* Information sharing modes
- *5.6.8* Success factors
- *5.6.9* Difficulties, information gaps, and community-defined coping mechanisms

[7] Beilock, S.L. (2007). Understanding, Skilled Performance, Memory, Attention, and Choking under Pressure. *Sport and Exercise Psychology.*

5.7 Aligning information technology with mission and workflow

5.7.1 Interplay between day-to-day and incident-focused operations in establishing situational awareness/common operation picture (SA-COP)

5.5 *What We Learned about the Community*

The Puget Sound maritime safety and security community is composed of a robust, mature, and diverse set of stakeholders with representation of organizations across the FSLTIPP. The Puget Sound area is unique in its large and diverse geographical area and international border that mandates a close partnership with Canada for management of the area's shared waterways. While in some cases, especially those involving specific incidents, the U.S. Coast Guard provides central operational leadership, on a day-to-day basis the community is not centrally managed; its practices are diverse and generally decentralized.

5.5.1 *Diversity*

There's so many organizations and all play a key role and a key function.
- A tug operator

The PSSSC is extremely diverse, and its organizations that are connected to one another in different ways — some formal and others not. Many of these organizations are in themselves large and complex, including individuals in different roles and with notably varied perspectives and experiences related to information sharing.

The theme of diversity of community participants can be understood within five frames:

1. Job roles
2. Views of responsibilities related to safety and security
3. Use of and access to information sharing technology/data
4. Home Rule
5. Leadership structures

1. Job Roles: The job roles held by community participants are varied. Security is thus a jointly realized effort among individuals in disparate occupational roles. The roles include those that are more obviously security related like law enforcement officers, intelligence analysts, emergency call center dispatchers, and first responders.

Other, less obvious, roles include facilities management, public safety officers, natural resource managers, and systems support contractors.

Different functional roles in the community lead to differences in understanding and practice. At the most basic level, perceptions of what security means and how information about it is shared are shaped by the various day-to-day missions and practices of community members. In our interviews, less than half (34 of 77) of the interviewees reported that their job role within their organization was primarily security related. Of the 34, only 4 interviewees said that their roles were 100% security related, while the other 30 indicated that their organizational role mixed security and other responsibilities.

This indicates that for the vast majority of community members, safety and security are generally part-time activities.

2. View of Responsibilities Related to Safety and Security: Within the community, participants define security and their responsibilities for it in many different ways. So, while security touches all sectors of the community in some way, organizations and roles are not responsible for or view security in the same way. Security needs are embedded in a wide range of responsibilities and contexts, leading to a high degree of variation in the perception of risk across the community as a whole.

Within the community, members continually work toward security aims in tandem with such diverse missions as securing access to a terminal, on-water fish and wildlife management, and event planning. Interviewees reported that as a consequence of this diverse tasking, cross-sector and cross-mission information sharing can be a particular challenge. For example, a U.S. Coast Guard Contingency planner described how differences in mission make it harder for organizations in different sectors to understand one another: “Ports operate under a business model, but government focuses more on citizen recovery. . . People don’t understand the authority of the Port.” Across the community, it is easier to share information across entities with similar functions, missions, and cultures.

. . . it is easier to share information because, like us, U.S. Coast Guard has a mandate for safety, they are civilian. . . but it is difficult under the security process to share information between different types of organizations. For example RCMP and Bellingham Police can share information because they are both law enforcement.
- Canadian Coast Guard

One way the community copes with this diversity is through formal and informal facilitators and interpreters who act as information leaders and work to integrate information across sectors and missions. These roles help the community cope with the challenge of bridging the many different perspectives on security. For example, many people in the community — such as public information officers (PIOs), Freedom of Information Act (FOIA) officers, and Fusion

Center personnel — have formal roles as interpreters and integrators of security related information. Regional organizations like the Marine Exchange and PNWER are also focused on this integrating role.

However, as we often heard in the interviews, several people do this type of connecting work much more informally. A number of interviewees indicated that they play this role based on their prior experience working at another maritime community organization. This cross-community experience serves as a foundation for good relationships and good information sharing with their former organization. For example, we interviewed a former US Coast Guard Captain who now works for a professional shipping association. He explained that he does not feel the need to attend regional USCG-organized drills because he knows he would "get a call from USCG if there were something going on." Similarly, the FEMA National Incident Management System (NIMS) officer is a former member of the U.S. Coast Guard and reflects that experience in his current job. It is not just that many community members have these prior roles that is significant, but that they bring them up in the course of describing how information flows and attribute successful information exchange to their connections from prior work experience. These experienced members of the community may be considered as cultural couriers between different organizations, and they reflect the importance of community self-knowledge.

> Cross-community experience serves as a foundation for good relationships and effective information sharing with community members' former organizations.

We may get reports from the public or from another city saying we saw this, somebody took this photo of this bridge so we'll send that. . . Somebody broke into one of the piers. We get that actually quite a lot.

- A county emergency manager describing how information flows through her organization to the WSFC

Safety and security actors also rely on a fair number of people and organizations as information resources, even though they are not generally seen as members of the community, *e.g.*, the Washington State Department of Natural Resources, which provides maps, and NOAA, which supplies weather-related information. Beyond this, the popular media were often mentioned as information resources during incidents, in some instances providing information faster than other community partners. Additionally, the general public was named as an information resource in several examples.

3. Information Sharing Modes: Another significant component of diversity stems from the many ways that information is shared during day-to-day work. Information is shared formally and informally, synchronously and asynchronously, remotely via technology and face-to-face. It may be secure or open, documented and distributed or of one-time use and off the record. The most frequently mentioned modes of communication employed in day-to-day operations are phone, radio, email, and face-to-face interactions. These modes of communication are in common day-to-day use across the community. However, individual entities also use a wide range of specialized communication tools to achieve situational awareness that are specific to their mission and their information sharing needs.

Of course there can also be a considerable degree of diversity introduced within each of these modes. Radios do not all talk with each other; a wide array of enterprise-level information systems lack interoperability or employ differing data standards. This diversity can be especially impactful where international partners are involved. The Canadian Coast Guard reports that its operational information management tool, INNAV,

> is more restrictive [than the earlier VTAS system] and creates a problem in language — INNAV calls it this, we used to call it this, and USCG calls it that. So we actually had to translate it between systems. But the translation table is more complicated with the new systems. Codes are different between the U.S. and Canada; how they describe vessels. Libraries don't match in the systems between the U.S. and Canada.

We mention here the varied modes of information sharing as an aspect of community diversity; an analysis of the use of these modes as an aspect of the ISE can be found below in Section 5.6.7 Information Sharing Modes.

> Information sharing is complicated by the use of numerous different communication modes. Even within a single mode (*e. g.*, radio), there is still diversity which may lead to interagency confusion or a lack of interoperability.

4. Home Rule: Adding to community diversity is the fact that Washington State is a Home Rule state. Under Home Rule, counties have broad authority to provide for purely local governance issues. Within the state, six counties, including key counties associated with the maritime community, have adopted home rule charters: Clallam (1979), King (1969), Pierce (1981), Snohomish (1980), Whatcom (1979), and San Juan (2005).[8]

Most states do not include emergency management in their Home Rule laws, but Washington State has determined that the charters do include emergency situations. As one emergency manager said, "You can have home rule laws for holidays, fireworks, etc. . . you can have all that. . . Any kind of plan or document that is integrated with

Then the State and Feds come in and say every situation will be handled using ICS, which is great, but because of Home Rule it isn't implemented the same way.
- Security consultant

[8] Municipal Research and Services Center. (2013). "County Forms of Government." Retrieved from http://www.mrsc.org/Subjects/Governance/locgov12.aspx#3

multiple agencies and multiple disciplines has rapidly increased the speed of my white hair," although she added, "There have been great advances in the last 10 years."

Home Rule status is viewed by many members of the community as supporting the tendency for day-to-day operations to be less formal and more fragmented. A U.S. Coast Guard Contingency planner said, "Being a Home Rule State means there is nothing that says everyone needs to abide by a regional support function," and the Washington State Department of Natural Resources said, "Because the state can't tell local areas what to do, we speculate that the success of Home Rule requires fragmentation." At the same time, Home Rule can also be viewed as providing greater flexibility.

We agreed to work through the county when responding to disaster because it is more efficient, but with Home Rule, we could arguably go through State.
- City director of emergency operations

Some differences justified by Home Rule stem from competition for resources. Funding requests go through the county, but because of Home Rule, local entities feel they still have the legal right to put requests directly to the State, and as a private security consultant put it, "they often do because they feel like if they don't go directly to the state, then the resources will all get allocated to Seattle, and then there will be nothing left for smaller entities/cities. They look at Seattle as the 'big gorilla.' Small cities think they have to beat Seattle to the punch; if they wait, then Seattle will get the resources and they won't get anything."

Home Rule status is viewed by many members of the community as supporting the tendency for day-to-day operations to be less formal and more fragmented.

5. Leadership Structures: Across the maritime community, structures for leadership are constituted in different ways corresponding to an organization's FISLTIPP category and its culture. While this results in considerable diversity, some sectors of the community, such as the enforcement sector or the private business sector, generally share similar structures. Our inquiry into the effects of leadership structures revealed that, on a day-to-day basis, key leadership relationships are based far more on years of prior shared experience than on formal organizational structures and agreements.

Three related issues are that (a) overall, formal leadership structures are clearer and more significant to the community during incidents than during day-to-day operations, (b) changes in leadership positions are an ongoing difficulty for the community, and (c) in day-to-day operations, leadership often falls to individuals who have knowledge and experience relevant to the work at hand, regardless of whether they hold a formal leadership role in their organization.

(a) Clarity and significance of leadership structures - In their day-to-day operations, members of the community work within the boundaries set by their individual organization's leadership structure. This invariably impacts the organization's operational ISE. The Puget Sound Pilots Association, for example, indicated that their personnel are arranged in a flat structure in order to produce an environment where everyone shares information.

Not surprisingly, the lines of authority and information sharing protocols are clearer and more significant in a post-incident scenario. This is due in part to NIMS, which was mentioned by some, but not all, of our interviewees. For example, air rescue associated with a county sheriff's office indicated that under NIMS they would yield to the U.S. Coast Guard for incidents on the Puget Sound, though they pointed out they had similar rescue capabilities. Similarly, FEMA stated that in the event of any incident where there is a request for federal assistance, they would participate in a unified command structure lead by the cognizant local, state, or federal command group.

However, interviewees indicated that there would be changes in leadership structure even for incidents that were not being managed under NIMS. For example, tribal law enforcement reported they would yield authority to local law enforcement in incidents where they were responding off tribal lands, and the Washington State Ferry system told us that in the event of a water-based response they would share information with the U.S. Coast Guard under the regional response plan.

(b) Effects of change in organizational leadership - As noted earlier in this report, many organizations within the community have leaders who have been in the community for decades. The relationships these leaders have developed over time offer an advantage as they make decisions about information sharing; they have background knowledge that guides their choices about who might be consulted when there are changes (*e.g.*, new regulations, new technologies) occurring in the community. Although the challenges associated with change in organizational leadership are well known to the organizations and are continually being addressed, they can present a challenge to organizations who work with the USCG with its regular turnover of key personnel.

It is going to have a big impact. I don't know what they're going to do. He is really THE guy you call when anything is going on. You pick up the phone and let him know.
- WSP speculating on the potential impact of an upcoming retirement in WSF

In organizations where the people occupying organizational roles change regularly (*e.g.*, USCG, USN), it takes considerable effort to ensure that relationships with individuals in other local organizations endure through the transition. Mechanisms to overcome the challenges include special efforts, such as introductions at community meetings and participation in regional training exercises. In instances where two organizations are culturally removed from one another (*e.g.*, U.SCG and an emergency call center), special agreements must be negotiated by the leadership structures to ensure appropriate information sharing across organizations, regardless of who occupies an organizational role at any given time.

In the case of international coordination, change of leadership can be especially difficult. While U.S. - Canadian coordination in this region is extraordinary, Canadian Coast Guard interviewees indicated that one troublesome issue was the difficulty of keeping track of who their counterparts were in U.S. Coast Guard, Sector Puget Sound.

> Changes in leadership and high turnover rates disrupt the personal relationships that the maritime community so heavily relies upon.

(c) Information leadership in operational context - In day-to-day operations, individuals accept the leadership of information leaders, who are not necessarily organizational leaders. Although individual organizations typically operate under a formal leadership structure, running parallel and complimentary to these formal structures is an informal system by which authority is bestowed upon information leaders, or individuals who have expertise in and knowledge of the work at hand. This means that leadership by information leaders is dynamic and may change as new projects begin and are completed.

Informal leadership structures operate 24/7 and neither these structures nor the role of information leaders disappear when an incident occurs. In fact, interviewees reported that during an incident, as soon as NIMS appears to slow or impede operations, people often default to working with information leaders and the informal leadership structures that support them outside of incidents. Thus, these informal leadership structures are an essential component of the community and are critical to the success of both day-to-day and incident-focused operations.

> The information sharing environment built during day-to-day operations is a critical component of emergency response and management.

We found concern in the community about the potential loss of key informal information leaders. As discussed earlier, many long-time members of the community, especially those who have worked in more than one community organization, have become central community information hubs. This includes a number of U.S. Coast Guard retirees who now work as civilians in law enforcement, private business, or the Federal Government. Here again the importance of community self-knowledge, gained through shared experiences and exposure to the culture and day-to-day operations of more than one organization, is revealed.

5.5.2 *Community of Doers*

WHILE diversity is a hallmark of the PSSSC, its members all pull together in the common effort to get things done. The members of the Puget Sound maritime safety and security community told us of many complex obstacles they face while carrying out their day-to-day tasks. Yet despite the many complications, the day-to-day operations of the community still generally manage to run smoothly. We found that this smooth functioning of the community is based, not so much on procedures and regulations, but on getting the job done through relationships and trusted communication.

The PSSSC is fluid, dynamic, and adaptive. If there is an obstacle that halts a process or mission, the members of the community do not reach for a manual, rather they reach out to one another to find a solution or workaround. Community members take it upon themselves to work with their trusted colleagues and get the job done. Sometimes this means that additional overhead tasks are introduced into the work process, and sometimes this means that processes are made more streamlined by adaptations — whatever the case, this community of doers finds a way to ensure the task at hand is achieved.

I'll take the initiative to go hey, do you know something? Is there something going on? Does it affect [my] County? Anybody I can send that to? I can ask that question.
- A county public information officer

5.6 *What We Learned about the Information Sharing Environment*

THE Puget Sound maritime community's information sharing environment is perceived by community members as having both positive and negative aspects; positive in that it is critical to work accomplishment, but negative in that it can open them up to risk. One risk that can have gaps or inhibit information sharing is competitive disadvantage.

5.6.1 *Competition*

Entities involved in commerce including the ports, terminal operators, shipping lines, tug boats, trucking companies, rail, and others operate in a competitive environment that exposes them to risk when business processes, information, or security vulnerabilities are exposed. If a specific port's security is seen as lacking, it can cost business. This risk is exemplified when a security consultant described information sharing in relation to "competition between terminals for business. . . Once it is found out that [they have] found something unsafe, they pull all their workers and go to a safe zone, and they stop production at the [port]. At this point, they don't tell Port Security or other terminals. . . By the time law enforcement came, that is when the neighboring terminal finally found out."

Additionally, resource competition among government and response organizations is a factor. According to another security consultant, "People get kind of protective [saying]. . . 'We don't want our partners to know what toys we have because then we will have to share'. . . Most of that stuff is funded by federal grant money and then it means they would have to share regionally."

Individuals, on the other hand, worry about being the one who shares too much, which can be a personal risk with professional consequences. This worry, as well as the overarching struggle with the risks of information sharing, was summed up in an informal meeting of intelligence professionals:

> Everyone's afraid of sharing information. They feel better if they can see the MOU but even if an MOU or law exists, if the organization does not have a developed relationship with another they are still hesitant to share information. No one wants to get blamed or set bad case law or be the one that gave too much. The willingness to share information increases with trust and familiarity with the other person and with the organization that the information was going to.

Relationships and trust go a long way towards mitigating competitive barriers to information sharing.

5.6.2 *Trust*

Effective information exchanges depend on established, trust-based relationships. On a day-to-day basis, information sharing is driven by the need to build and maintain lateral relationships across a diverse set of stakeholders. Many interviewees described trusted relationships as the precursor to successful information sharing and resource alignment needed for effective incident response. The Puget

Sound Pilots expressed a desire "to know the Coast Guard people as much as possible so they can trust [us] when [we] talk to them" and credit their current "great relationship" with the USCG for smooth information sharing. The Marine Exchange and others hire retired USCG officers for this reason.

Building and maintaining relationships among partners is ongoing work in the community. When policies and procedures need to be worked out or altered, informal information sharing and trust building are viewed as key to working out information needs and establishing long term joint agreements. Such agreements sometimes remain informal and are sometimes formalized through MOUs or other mandates. Meetings, conferences, and face-to-face interactions are viewed as particularly helpful for establishing trust and relationships. When good relations exist, problems are reported and resolved more quickly.

> Trust among community members is the foundation of effective information sharing. Trust encourages information sharing, increases the likelihood that shared information is considered valid, and precurses formal agreements. Trust must be continuously built and maintained.

5.6.3 *Clearance Levels*

Security clearances are a means of including individuals in or excluding them from information exchanges. The national security classification system[9] governs all national security information generated by the U.S. Government, its employees, and certain external sources. The process for obtaining a clearance under this system and for gaining access to classified information within the system is formal and well-controlled. Access to classified information is authorized by an individual's clearance level and by their need to know.[10] Thus, a Secret clearance does not grant an individual access to all Secret information but only Secret information required for them to carry out their work.

Outside the national security domain, a series of additional designations, such as Law Enforcement Sensitive, Personal Identifying Information, Sensitive but Unclassified, and For Official Use Only further limit access to information. Guidelines for admitting individuals into such information compartments and for designating information that falls into such classification groups are less formally prescribed than those in the national security classification system. An information

[9] The national security classification system has designations of Unclassified, Confidential, Secret, and Top Secret.

[10] Need to know is established through compartments. Access to compartments is granted to individuals in addition to their clearance level.

technology system has to account for the specific information attributes assigned to the piece of information and for the individual who wishes to access that information.

The barriers attributed to classification relate to efforts to develop a shared operational picture, which often requires integrating information that is drawn from classified and unclassified sources. Other instances concerned difficulty in processing or handling the movement of classified or sensitive information, such as the need for specialized equipment. Many instances represent cases where one or more parties want to share or receive a particular piece of information but are prevented from doing so because they lack the clearance needed to be a recipient of that information. In some cases it was mentioned that clearance is hard to get.

> While interviewees acknowledge there are legitimate reasons for restricting access to sensitive information, they frequently mentioned classification of information as a barrier to information sharing across partners.

Specific information challenges attributed to lack of clearance include the inability to answer "what the threat is to us," inhibition of work flow and/or delays in information flow between partners, "gaps in who is fully informed," and restrictions in who can participate in exercises. The Bainbridge Island Police Department confirmed some of these challenges as they described the "sticky water of security clearance that causes delays in [them] getting needed information." For some, the difficulty concerns weighing the risk associated with information sharing against who needs to know or who should know. These issues were ambiguous for many interviewees and generally not aligned with the informal, trust-based operational ISE. We heard many stories of classified information being informally shared, inappropriately according to the formal national secuirity classification system, to get important security work done.

5.6.4 The Relationship between Day-to-Day Operations and Incidents

Another thing we learned is the important relation of "incidents" to day-to-day operations. While our interviewers explained MOISA's focus on day-to-day operations, interviewees still often offered examples of information sharing related to incident response along with those of day-to-day activities. Focusing on day-to-day operations does not diminish the importance of incidents, but it does provide a different perspective on them. For many interviewees, their day-to-day operations support incident management either directly, when various levels of incidents occur on a regular basis or indirectly, when day-to-day operations are motivated by the ongoing risk of potential incidents. It is in this latter sense that the safety and security community is also a community that contribute to regional resilience.

The point at which an event becomes an incident is not clear and is often a matter of perspective. 9-1-1 dispatchers spend their days fielding calls from people in crisis, yet their perspective on the events reported to them is very different from that of the person calling in. A U.S. Coast Guard planner may spend much of her day developing plans for responding to incidents, but that is still her day-to-day work.

> From the perspective of day-to-day operations, security is not simply ’switched on’ in the event of an incident but rather is something that is continually being refined and maintained and exercised.

Security is a service that the community works hard to provide every day, 24/7. Viewing security as an ongoing service means that day-to-day operational information sharing is typically driven by an awareness of possible incidents, but this differs from information sharing in response to a specific already-occurring incident. Achieving security to support societal and economic resilience requires constant activity to build and maintain the relationships and resources that become essential when incidents do occur. When security is viewed this way — as a continually available utility — it becomes evident that resilience is accomplished not so much through formal top-down command structures for major incident response, like NIMS, but rather through the distributed, localized, day-to-day operations of community members. This arrangement is viewed, for example, as aiding the speed and quality of search and rescue missions and other joint efforts.

[In our SAR plan there is] no interference from DC and Ottawa. We can conduct SAR missions without clearance. Rescue centers can determine between U.S. and Canada who has the best resources to send and who should take the lead. The authority lies at the regional rescue coordination center.
- Canadian Coast Guard

> The work of aligning the resources and building the capability to respond to incidents occurs outside of the context of an incident.

One Public Information Officer (PIO) remarked that part of her day-to-day work involves meeting and “getting to know” other PIOs because in the event of a disaster, these are the people she will need to work with. Although the work she is describing differs from what she would be doing during an incident and occurs outside of any specific incident, it is still very much driven by her desire to prepare for a future incident.

Right, so during a disaster we would be setting up a JIC a joint information center and I need to know all the other information officers in the county so I can draw upon them to help, you know during disaster kinda stuff, and then we get together on a regular basis just to get to know each other.
- A county public information officer

Both the complexity of the ISE and the complexity of sharing information associated with multiple stakeholders means that successful information sharing requires expertise in the community itself. On an individual basis, such expertise is described by many interviewees as taking years to build. Impressions of capacity and collaborative ability of partners may also build up over the course of years. The community has many coordinating mechanisms and processes in place — both formal and informal — to facilitate successful partnerships. Maintaining the coordinating mechanisms and processes that successfully align partners and build relationships is often a long-term and ongoing process (See Regional Coordinating Mechanisms as an Information Sharing Sucess Factor in Section 5.6.8).

Successful information sharing requires expertise in the community itself.

5.6.5 *Formal versus Informal Information Sharing Practices*

In our literature review, we found that informal practices are underrated as significant drivers of day-to-day safety and security information sharing. Unlike the literature (*e.g.*, GAO reports), members of the community generally discussed the critical importance of experience and the development of trusted relationships as the key elements driving their information sharing behaviors, not formal procedures or legal authority. Even when there is legal authority regulating interactions, the complexity of ongoing field operations means that the day-to-day activities of the community still tend to be individualized and generally informal.

The only formal written agreement is the Area Maritime Security Plan (AMSP), but who actually reads it? It is a strategic overview for recovery but there is no signature line. It's classified, so many of the folks I work with don't even have access. Outside the maritime community, no one has read it and they don't have the security clearance, anyway. The USCG planner says there is value in having the plan, but so many key local people have no awareness of it and make their own plans. *Then their plans affect your plans, but neither side knows what to expect. There is no 'intermodal awareness.'*
- USCG planner

The lack of formality seems to extend across the community, even including key federal and international partners. For example, an administrator of the Washington State Ferry system explained that there is "not a formal system to get information — even with U.S. Coast Guard." As he explained, his office receives informal requests from "U.S. Coast Guard maybe 10 times a year to ask a question" via telephone. Their offices had "worked together for 10 years with no formal requests."

Similarly, members of the community explained that even a system as formally defined as NIMS or other federally-mandated plans like the Area Maritime Security Plan (AMSP) are implemented variably at the local level and do not necessarily make it easier to coordinate at the local level. As a state emergency manager pointed out, "Washington State counties and numerous local organizations do things differently. Then the State and feds come in and say every situation will be handled using ICS, which is great, but it isn't implemented the same way." Even for the military, regional day-to-day operations are far less formal than they are perceived at headquarters. One naval officer explained, "requirements come down from national regulations, but they are handled and implemented locally."

At the international level, even national policies can give way to local, less formal processes that are flexible enough to change easily over time. Regional U.S. and Canadian Coast Guard operators jointly maintain an operations manual that is reviewed and modified as required at meetings that occur twice a year. This manual is shared between the two countries and evolves without the requirement for constant review or approval of the two governments.

MOUs, MOAs, and Other Formal Agreements: Formal agreements within the community typically take the form of Memorandums of Understanding (MOUs) or Memorandums of Agreement (MOAs). When these formal agreements were discussed, interviewees' perspectives varied greatly. The impact of MOUs/MOAs on day-to-day information sharing in the Puget Sound region is difficult to assess because interviewees' reports regarding the impact of MOUs/MOAs varied, ranging from positive to irrelevant.

MOUs/MOAs are put in place for a variety of reasons, such as to get the approval required to begin collaborative, grant-funded projects, or to establish rules for sharing physical resources and equipment. Several interviewees mentioned formal agreements specific to information sharing, and all but one of these instances were in reference to agreements between or among federal and state government organizations. Although there is value in the flexibility that arises out of informal interactions and day-to-day operations, interviewees also recognize the value of formalizing some relationships. MOUs/MOAs are seen as (1) useful, in some cases, and (2) not helpful or relevant in other cases.

Everyone's afraid of sharing information. They feel better if they can see the MOU but even if an MOU or law exists, if the organization does not have a developed relationship with another they are still hesitant to share information.

- Comment at an informal meeting of intelligence professionals

(a) MOUs/MOAs are useful - When asked if she had an MOU that she relied on for information sharing, a county emergency manager stated,

> We do, and actually it's a wonderful resource that's available on our website. We have what's referred to as an RCF (Regional Coordination

> Framework for Disaster and Planned Events). It had a previous version called the Regional Disaster Plan (RDP). This was created in the late 90's before there was the Washington State Intrastate Mutual Aid System (WAIMAS). So it was our documentation for mutual aid partner-to-partner. What makes it unique and different from any other formal mutual aid process is that it does include private and non-profit. So it outlines how we do situational awareness, how we do public messaging, how we make regional policy decisions.

MOUs/MOAs may establish rules for information sharing along multiple dimensions: the content of the information, the mode by which it is shared, and the equipment required to transmit or receive the information. MOUs/MOAs help maintain continuity of information sharing relationships between organizations with high turnover, such as the U.S. Coast Guard, and serve as resource documents for new people coming onto the job. In some cases, MOUs were cited as reinforcing charters, and in other cases, MOUs were described as unnecessary because existing charters and or/mission statements covered all needed relationships.

While MOUs can help formalize trust relationships between entities to maintain the continuity of the relationships and to help ensure that they feel more comfortable sharing information, the benefit of formal agreements requires that the parties have a relationship beyond the specific elements documented in an MOU or MOA.

> The benefit of formal agreements requires that the parties have a relationship beyond the specific elements documented in an MOU or MOA.

(b) MOUs/MOAs are not helpful or relevant - Interviewees frequently reported not knowing of any existing MOUs that involved their organization. Others reported knowing of existing MOUs, but stated that these were not important because effective nuanced information sharing is governed more by personal relationships. A County public information officer stated:

MOUs are *pieces of paper that don't do anything.*
- City Fire Chief

> I have a lot of MOUs but most of them are for providing resources and assistance. I can't think of any MOUs that I have for information sharing. I think it's the way it's worked so far and we have really good relationships with our city officials, with the Navy, with the bigger companies like Puget Sound Energy. So we have these kinda, it's the old networky thing. If you know who you're talking to, you can feel comfortable going: alright, I'm going to tell you this much, but this I'm not sure of, so don't say about this until I'm sure.

Many pointed out the advantage of trusted, informal information sharing over formal, mandated sharing, is that it can be nuanced in useful and flexible ways. One public information officer gave an example when she said to us "I'm going to tell you this because I know you won't share or tell where you heard it."

Other interviewees talked about problems that arise when different organizations and different people within an organization interpret MOUs differently. One interviewee discussed an MOU that was ignored because it required entities to interact in a way that was counter to how things had historically been done.

An interviewee from one of the tribes reported wanting an MOU with neighboring law enforcement, but that achieving MOUs/MOAs between tribal and non-tribal entities is very difficult. Several interviewees reported that potential partners may be hesitant or unwilling to enter into MOUs/MOAs because they see an MOU as an unwanted responsibility. Another interviewee explained that organizations may be more willing to sign an MOA rather than an MOU, because MOAs are "a little less formal."

Policy and Liability: Another aspect of the formal/informal tension experienced by the PSSSC is realted to policy and liability. These issues were often cited as hindrances to information sharing. Some State level officials, for example, report being wary of maintaining or sharing information that could be used by local entities for their own purposes. As a representative of the Washington State Ferries stated, "There are good reasons to do work informally... If you make certain things policy, your hands are tied to work and share information in a certain way."

Formal communication can become tangled in privacy issues and information access policy, which can reduce the information's value through redaction or slow the flow of information. A Washington State Fusion Center (WSFC) employee reports that

> Privacy policies are a source of frustration... Privacy policies are a key driver of activities, specifically, ensuring that WSFC respects American civil liberties, first amendment rights, and complies with 28 CFR Part 23.

The WSFC spends considerable energy trying to understand how they need to act in accordance with different privacy policies and they always err on the side of caution. Whenever they doubt whether a certain activity (typically collecting and sharing intelligence) is allowable, they will not engage in the activity. For example, compared to federal privacy policies, Washington State's policies are more restrictive when it comes to gathering intelligence, but less restrictive when it comes to sharing information with the public.

Information ownership affects access. When asked about how law and policy affect the way information is shared, a local police

The Washington State Department of Natural Resources (DNR) has an MOU with the EMD (State Emergency Management Division) to be the advisor on all land issues, but because the DNR is not a governor's agency, communication often goes through other of the Governor's agencies, like the Department of Ecology.
- WADNR geologist

I use my work phone for work business, but occasionally use my personal cell phone too. Sometimes I do this to avoid my work phone records being requested as part of public records requests.
- A port security manager

I share information based on relationships, not policy.
- A port security manager

WSFC workers are technically employed by different organizations (i.e., the City of Seattle, the Washington State Patrol (WSP)) that have different laws and privacy policies. In cases where there are multiple, different privacy policies, the WSFC bends to the most restrictive policy.
- WSFC interviewee

FEMA uses information sharing platforms called Web-EOC and HSIN. There is a lack of policy and guidance on how to conduct information sharing. There are a lot of tools, but not much guidance.
- USCG District 13

chief responded, "It depends on who holds the database. If it is the feds, then sharing is not good, but if it is mine, then I will share with anyone." Technology solutions designed to impose uniform information sharing policies have not thus far been considered very effective because, in some cases, there is limited buy-in and guidance on use.

Finally, liability associated with formal requirements for use of information can slow or stop the flow of important security-related information. The issue of liability associated with legal access to information was especially prevalent in comments about barriers to receiving information from the WSFC.

People are afraid to coordinate because they don't want to break rules they aren't aware of. They aren't clear as to policy on who to share with and what to share.
- USCG planner

As a city emergency manager explains: "The Fusion Center has to wait until CNN comes out with stuff. . . They won't tell the EOC anything because it may be an ongoing investigation. . . A day-to-day analysis and threat picture is not there. They are late to the game on telling people obvious information. . . Their role is not well-defined. . . They produce a yearly assessment that is poorly done. . . Threat assessment is a weak area."

5.6.6 Information Sharing with the Public

Our examination of day-to-day information sharing found that the public is weaved through the maritime information sharing environment in multiple ways. Calls from the public are often where an incident begins. Volunteer organizations such as CERT (Community Emergency Response Teams), the USCG Auxiliary, and ARES (Amateur Radio Emergency Services) can be integral to community activities, requiring, shaping, and providing information. Several interviewees mentioned media as an information resource during events. Others mentioned the role that sunshine laws and policies play in shaping information access to the public and informing how they share information with partners.

5.6.7 Information Sharing Modes

As mentioned, day-to-day information sharing takes place across several modes of communication. Modes frequently mentioned in relation to day-to-day operations include phone, radio, email, and face-to-face interactions.

Modes are often mentioned in tandem, suggesting that accomplishing a given task often demands turning to multiple kinds of information resources.

Figure 5.2 shows the distribution of modes that were mentioned in the course of PSSSC descriptions of of sharing information. "Mode not specified" comprise instances of information sharing in which no specific mode was referenced. "Other" comprises modes mentioned very infrequently. Interviewees described using more than one mode in association with one instance of information sharing; therefore, the percentages do not equal 100.

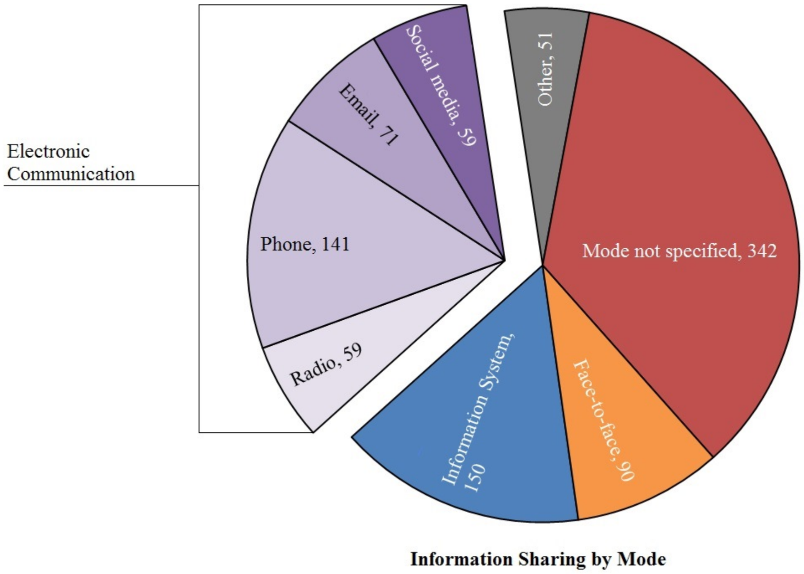

Figure 5.2: Information sharing by mode.

Face-to-Face Information Sharing: Interviewees viewed face-to-face communication as a major mechanism for accomplishing the work of aligning resources, building joint capacity and a shared operational picture, strengthening relationships among individuals and organizations, and professional development. Many attributed face-to-face communication to building the trust needed for successful information sharing.

Face-to-face communication — which includes meetings, conferences, and joint exercises and drills — is highly valued by the community.

Electronic Communication Technologies: Modes in this category include phone, radio, email, and social media. Smart phones used for email are included in our analysis of email, while those used for other applications are considered along with information systems.

A particular feature of maritime communication is that it makes extensive use of radio communication for day-to-day operations, incident response, and security functions. One tug boat operator described how he uses radio to share information:

> [Communication with the] Marine Exchange is done via that VHF radio which is Very High Frequency within our boats, and they monitor channel 20 so you can call down and let them know what you're doing. All the bridges are on channel 13 so you'll do that. Coast Guard monitors channel 16 and it's recorded 24/7 so if there's an emergency, you make sure you have the radio on 16 and you say things: your time, your position. So a lot of it can be done, a good portion of it can be done through the radio whether it's your traffic, [communication with the] Marine Exchange, bridge-to-bridge, or calling a bridge.

I know I'm aging myself, but [social media is] the next step up from the scanner, where people used to listen to the scanner and they still do, but listen what was going with the police and what was going on with the you know with fire, and I'll tell you, police use their Twitter accounts really well. Washington State Patrol really uses it well. I mean there was one Twitter where um G.G. was on there, just giving updates of, it was, we had a mass [shooting]. . . So, it was discussion of that and trying to find that car (the car of the perpetrator). . .
- A county public information officer

We prompted interviewees to tell us about social media use in their work, yet social media was not mentioned frequently in relation to day-to-day operations. However, it is being increasingly used by some interviewees and their organizations, some of whom are employing it to push information to the public and expand situational awareness.

Public information officers in the community specifically cultivate training and sharing of best practices on social media. Interviewees pointed to the Washington State Patrol, some local emergency management PIOs, and fire departments as notably effective at social media communication.

While information sharing investments are often focused on information systems, our data reveal that more generic communication technologies such as phone, radio, and email remain the "primary channels" for information sharing in the community.

5.6.8 *Success Factors*

The above sections describe an ISE that is very dynamic and complex, yet interviewees were more likely to describe information sharing practices that are working than to discuss information gaps or difficulties. Although such difficulties do exist (discussed in Section 5.6.9), in this section we discuss the most prevalent intangible (*e.g.*, trust) and tangible (*e.g.*, grant-funded collaborative group projects)

Interviewer: *Do you experience any information sharing barriers?*
Interviewee: *We don't usually have to ask for information because we have been working with the community for a long time so information is pushed because the need is recognized.*
- Washington State Ferries employee

factors that help community members successfully navigate the complexity of their ISE.

Trust as an Information Sharing Success Factor: Time and again, when asked about information sharing practices with partners, interviewees answered in terms of the quality of the relationship. Where a shared understanding and joint trust were perceived to exist, interviewees reported no or few problems with information sharing. For example, one interviewee reported that an information sharing partner preferred to go to an organization with which they had a strong organizational relationship over one that had more accurate information. Thus trust and a shared understanding can be considered two qualities of a relationship that greatly influence the success of information sharing, slowing or stopping the information flow when not in place and aiding the flow when in place.

> Lack of trust is a bottleneck or even a barrier to information sharing. Even when formal processes are clear and established, interviewees reported that lack of trust would hinder the flow of information.

Regional Coordinating Mechanisms as an Information Sharing Success Factor: Coordination and collaboration among a diverse set of stakeholders is critical to the success of safety and security operations. In this section, we describe some of the mechanisms by which this coordination and collaboration are achieved. Many of the coordinating mechanisms that enable the success of key business processes in the community span the distinction between day-to-day and incident focused operations. Chief among these are activities that emphasize face-to-face interaction including exercises, joint planning meetings, committees, and working groups.

Regional coordination mechanisms serve distinct purposes and roles in information sharing depending on the degree of formality of the activity (formal/mandated vs. informal/voluntary) and the activity’s funding status. Formal or mandated coordinating mechanisms are generally ongoing and often unfunded. They typically focus on response planning and the long-term maintenance of regional security. In contrast, many of the voluntary activities are shorter term and, being project-based, are often funded. The degree of formality and funding status of the activity impact the types of stakeholders involved, including non-maritime stakeholders from land and air transportation. For example, Pacific Northwest National Laboratories hosts dockside drills under the Port Security Grant Program-funded radiation/nuclear detection program, yet participation in these drills by federal employees can be hindered by funding restrictions on federal employees getting paid overtime to attend. Also, participation by smaller entities is hindered by funding and staffing issues.

Mandated coordinating mechanisms - Prominent among the mandated activities in the region are meetings of the Area Maritime Security Committee (AMSC). The AMSC was established under the Maritime Transportation Security Act (MTSA) on 25 November 2002.[11] The Puget Sound AMSC meets quarterly, with associated executive and committee meetings. The AMSCs were established under the MTSA to provide a formal link for contingency planning, development, review, and update of the Area Maritime Security Plans (AMSP) and to enhance communication among port stakeholders within federal, state, and local agencies and industry to address maritime security issues. The U.S. Coast Guard Sector Commander — the Captain of the Port — chairs the AMSC. Other committee members include representatives from port facility security, port operations, ferries, FBI, Seattle Police Department (SPD), Marine Exchange, Army, Washington State Patrol, and commercial businesses.

Additional formal/mandated coordinating mechanisms include procedural and administrative meetings to manage the Standard Operating Procedures in reference to U.S. and Canadian Vessel Traffic in the Juan De Fuca Strait.[12] To manage shared waterways, the U.S. and Canadian Coast Guards have established procedural and administrative meetings that meet bi-annually to revise and update, as necessary, the standard operating procedures that both entities utilize to manage the waterways under CVTS. National and international regulations designate which vessels must participate in CVTS. Rules for CVTS participants are spelled out in the Canadian Radio Aids to Marine Navigations (Pacific and West Coast) and the U.S. Coast Guard Vessel Traffic Users' Manual.

While less focused on maritime issues, FEMA Region X holds Regional Interagency Steering Committee (RISC) meetings. These formal meetings include representatives from state, local, and Federal Government agencies. RISC meets quarterly rotating through each of the four states that comprise FEMA Region X[13] to enable representatives from smaller local agencies who do not otherwise have travel budgets to attend periodically. The RISC is designed to foster partnerships among agencies and to coordinate interagency and intergovernmental planning and response to disasters. Representatives from FEMA Region X and partners from other agencies meet regularly to enhance the federal, state, and local governments' ability to work in concert when it comes time to respond to disasters.

[11] Maritime Transportation Security Act of 2002. Public Law 107-295, 107th Congress. Page 116 STAT. 2064.

[12] In 1979, by formal agreement, the Canadian and the United States Coast Guards established the Cooperative Vessel Traffic System (CVTS) for the Strait of Juan de Fuca region. The purpose of the CVTS is to provide for the safe and efficient movement of vessel traffic while minimizing the risk of pollution by preventing collisions and groundings and the environmental damage that would follow.

[13] Alaska, Idaho, Oregon, and Washington

Voluntary coordinating mechanisms - We observed differences in the voluntary and mandated coordinating mechanisms with respect to the types of information shared and the types of stakeholders who attend. Information shared at voluntary mechanisms is typically related to day-to-day operations, whereas information shared at mandated activities is typically strategic, tactical, or policy-related. The majority of the attendees at the mandated coordinating mechanisms listed above are representatives from state, federal, local, and tribal governments, with a focus on the maritime domain. In contrast, many voluntary activities include participants from both the public and private sectors whose area of operations spans both the land and the maritime domains — types of entities that are reportedly difficult to engage in the information partnerships that are key to successful collaboration. The inclusion of land and maritime partners is particularly apparent in activities that focus on the movement of an entity across the boundary between land and sea.

An important example of a voluntary coordinating mechanism that facilitates information exchange is the Puget Sound Harbor Safety Committee (PSHSC). The PSHSC, chaired by the Marine Exchange of Puget Sound, is a professional group that meets bi-monthly to identify, address, plan for, and communicate safety and security issues within Puget Sound. Unlike the AMSC, which is mandated by the Safe Port Act and is not specifically funded, the PSHSC is not mandated and is a non-profit organization.

Information shared at PSHSC meetings is typically focused on how to improve the safety and security of day-to-day operational activities, whereas information shared at AMSC meetings is somewhat removed from operations and more focused on potential threats and long-term planning.[14] Some stakeholders who are primarily concerned with day-to-day operations expressed that this is a factor in some private and professional stakeholders' reluctance to participate in AMSC.

In contrast to the AMSC, which is primarily composed of stakeholders representing government entities (federal, state, municipal, and tribal), the majority of attendees at PSHSC meetings are from private organizations, both commercial and professional. About half of these businesses have a clear maritime focus, while the other half are mixed, focusing on both maritime and land-based operations. Stakeholders with a mixed land and maritime focus include private companies whose business depends on the intermodal transport of goods across land and sea, public ports with intermodal transport yards, and government entities with a land and maritime area of responsibilty such as the Department of Fish and Wildlife, and the U.S. Army Corps of Engineers. The majority of stakeholders with a

[14] Government Accountability Office. (2006). Maritime Security: Information-Sharing Efforts Are Improving. (GAO Publication No. GAO-06-933T). Washington, D.C.: U.S. Printing Office.

mixed maritime/land represent the petroleum industry (Shell, BP, Tesoro, Maxum Petroleum). Also present at the PSHSC meetings, but not present at AMSC meetings, are representatives from various professional organizations, environmental interests, and labor unions (*e.g.*, Marine Carriers Council, American Waterways Operators).

While PSHSC meetings include participation by entities often not found in regional mandated activities, neither the U.S. Navy (USN) nor the U.S. Maritime Administration (MARAD) attend PSHSC meetings on a regular basis, despite active recruitment by the PSHSC for such representation. In response to a question about why the Navy is not present at these meetings, one naval officer said that he "doesn't feel a great need for the Navy's involvement in these meetings." The low participation by the USN and MARAD may also have to do with geography. There is only one MARAD officer for a very large geographic area that extends beyond the Puget Sound, and he or she may have numerous competing commitments. The USN base is some distance away from where the meetings are held, and attending is a whole day commitment.

Unique among the voluntary gatherings is the Maritime Intelligence Group (MIG), which meets regularly near the northern U.S. border and comprises representatives from U.S., Canadian, and tribal governments. The MIG provides a compelling example of an international group of security professionals who have established trust relationships that enhance the safety and security of our region by meeting informally on a voluntary basis and thus mitigating barriers to international information sharing. This informal international professional group grew out of partnerships that were developed to coordinate the 2010 Vancouver Winter Olympics. The group was originally housed in the 2010 Olympic Marine Operations Center, which was officially disbanded after the Olympics event. However, the group saw a need for an ongoing partnership, and with no other existing mechanism, they continue to work together under the MIG.

Engaging Intermodal Stakeholders: Engaging land and air partners in the maritime ISE is a challenge that needs to be addressed. Through our analysis of radiation/detection exercises, we learned that the distinction between land and water is not always useful, as resolving threats on the water necessitates coordination with entities that do not have a maritime focus. Land and maritime-focused agencies conduct separate radiation/nuclear detection exercises; through our attendance at these exercises, we found that the events should be conducted jointly in order to practice transitioning responsibility from maritime to land-based security entities in the event of a threat.

Interviewer: *What would you say about the relationship between maritime and rail?*
Interviewee: *Nonexistent. Rail is really good, but to get them at the table is RARE, really rare. They have their process nailed down. They know what's on that car and they can tell you what's on that car.*
- A security consultant

One interviewee from a professional shipping association pointed out the vagueness of distinguishing land from maritime entities: "When we talk about maritime domain awareness, what do we mean by maritime? Some people think maritime is fishing, some people think it is recreational boaters; some people think it is U.S. Coast Guard." This interviewee complained that the Governor's maritime plan only related to fish processing. It had nothing to do with cargo, imports, exports, or manufacturing. He also commented that "people wonder whether to include the land when talking about maritime."

One way the region addresses this challenge is through activities that focus on transportation or operations that support movement across the boundary between land, air, and sea.

SPOC (Seattle Police Operations Center) actually had Fire people co-located. Ferry has [their] own plan — there is a split between maritime and land, and it needs to be better coordinated.
- Seattle Fire Chief

Several events organized by the Pacific Northwest Economic Region (PNWER) play a prominent role in organizing intermodal and cross-boundary activities in our region. One example is the Regional Maritime Transportation Recovery Exercise. In 2011, President Obama and Canadian Prime Minister Harper established the Beyond Border Initiative, which established a cross-border partnership focused on perimeter security and regional economics. The Initiative directed Transport Canada and the U.S. Coast Guard to oversee the development of a Perimeter Security and Economic Competitiveness Action Plan. PNWER was selected to facilitate the working groups, the development of the U.S. portion of the plan, and to facilitate exercises within the area. The most recent event took place in August 2013 and attracted 114 participants including representatives from regional ports, multiple local, state, provincial, and federal agencies, and a broad spectrum of entities including transportation, manufacturing, large importers, tug and barge companies, and shipping companies. Business sector participants were as diverse as Holland America, Boeing, Starbucks, AT&T, and Cloud SafetyNet. The Lummi Indian Nation also signed onto the project.

Other meetings, such as the PSHSC, which have high participation from land-water based and private sector entities, frequently feature intermodal transportation security topics. For example, two of the four PSHSC meetings in 2014 featured presentations about the Washington State Department of Ecology's project to analyze risks associated with the movement of crude by rail and the changing energy picture.

In the Phase 3 section of this report, which focuses on the movement of cargo from an international vessel through a domestic terminal and onto a truck for transport, we further explore this phenomenon; by focusing on the work required to maintain the security of things transiting between land and sea we learn about otherwise hidden and sometimes difficult to engage stakeholders.

When we get grant funding, the focus is on seeing who is out there, who we might want to work with, and what we can do.
- Emergency Operations Center Response employee

Project-based Collaborative Groups and the Development of Communities of Practice: During an informal visit to the Washington State Emergency Operations Center, an Emergency Operations Center Response Chief pointed out that collaborative group projects are critical to getting to know potential partners, their strengths and weaknesses, and the strengths and resources of their organization outside of an incident. Under a short-term grant funded project, he gave an example of how he worked with the Washington State DNR, FEMA, the Western Washington University's Institute for Resilience, and a contractor to create the Seismic Scenario Catalog.[15] Based on the success of this collaboration, he sought funding to work with some of the same collaborators to create the Resilient Washington Report.[16] Later, when the Oso mudslide disaster occurred in March 2014, he found himself working with some of the same people as part of the response effort, and having had the experience working together on two previous projects improved their ability to come together to handle the incident.

There is considerable research in project-based learning and project-based management that suggests that collaborative group projects support the development of broad interdisciplinary communities of practice. A community of practice is an emergent "mechanism where ideas and practices spread in work settings" that typically exists outside the normal work hierarchy and transcend organizational boundaries. Ayas and Zeniuk[17] explain how project-based collaboration builds such mechanisms:

> Membership in projects is temporary and thus offers individuals the opportunity to belong to multiple communities. In project-based organizations, there are a large number of weak ties that help diffuse knowledge and practices. In the majority of organizations, project members maintain their links with their functional departments (where they will return upon completion of the project if they are fully assigned to it). Membership in multiple existing communities contributes to creating informal webs of people who act as knowledge brokers. Project based organizations thus enable a continuous building and cultivation of relationships, nurturing the development of 'communities of practice.'

Port Security Grant Program (PSGP) funding plays a significant role in bringing together community stakeholders to collaborate, frequently in the form of grant-funded project-based working groups. Two recent examples of technology-oriented PSGP projects that have established such working groups are the *Maritime Common Operating Picture* (MCOP) project and *FirstToSee*. MCOP is designed to act as a portal that links multiple SA-COP systems, many of which are already in use at various local organizations.[18] *FirstToSee* is a platform and app that harvests incident-related Twitter data as

[15] WADNR, Washington Military Department EMD, WWU Huxley College of the Environment, FEMA, USGS, URS Corporation. (2013). Washington State Earthquake Hazards Scenario Catalog. https://fortress.wa.gov/dnr/seismicscenarios/

[16] Washington State Seismic Safety Committee, Emergency Management Council. (2012). Resilient Washington State: A Framework for Minimizing Loss and Improving Statewide Recovery after an Earthquake. Olympia, WA.

[17] Ayas, K. and Zeniuk, N. (2001). Project-Based Learning: Building Communities of Reflective Practitioners. *Management Learning*, 32: 61.

[18] The MCOP Working Group, which is led by Seattle Police, includes U.S. Coast Guard, security officers, Fire Department, Police search and rescue, ports, emergency operations centers, and the Marine Exchange.

well as eye-witness reports from private citizens to give responders an up-to-date, boots-on-the-ground picture of incidents as they unfold.[19] In both of these cases, however, we found concerns about the impact of PSGP's policies on the effectiveness and success of these project-based collaborative groups.

5.6.9 *Difficulties, Information Gaps, and Community-Defined Coping Mechanisms*

While we found that much of the community's desired or expected information sharing is occurring without obvious difficulty, there are some persistent community-identified challenges associated with information sharing that shed light on opportunities for improving their ISE. Interviewees were specifically asked if they experienced any information sharing difficulties, barriers, or gaps, so it is not surprising that information sharing difficulties are discussed in 64 of the 69 Phase 1 field observations and interview events. A few of these challenges are related to technologies (*e.g.*, radio frequency misalignment), but many more are not technology-based.

Washington is unique — we work really well together, we network and communicate. We know each other's capabilities. We train together. We play really well in the sandbox together. Of course, 'everyone has their lanes. . . it's not perfect.'
- Program Manager from Washington State Department of Health, Office of Radiation Protection

The Importance of Technology in Addressing Information Sharing Difficulties: As noted earlier, we identified 795 examples of information sharing in the Phase 1 field note data. Interviewees offered three types of information sharing events: (1) high level descriptions of their day-to-day practices, (2) detailed and specific examples of an occasion of information sharing, and (3) hypothetical scenarios such as how information would be shared with a particular partner during a particular kind of incident.

Where operational information sharing difficulties were identified, technology solutions alone would appear to address only about 10%. Of the 795 examples of information sharing, 296 were identified as having some difficulties associated with unmet information needs. The difficulties associated with those unmet information needs were classified into one of three categories: (1) difficulties attributed to ICT only, (2) difficulties attributed to non-ICT difficulties, or (3) difficulties attributed to both ICT and non-ICT difficulties:

1. 10.5% were coded as difficulties attributed to ICT only.
2. 55.2% were coded as difficulties attributed to non-ICT difficulties.
3. 34.3% were coded as difficulties attributed to both ICT and non-ICT difficulties or an interaction between those two categories.

In other words, initial analyses indicate that the vast majority of information sharing difficulties do not derive from solely IT causes.

[19] The *FirstToSee* project is led by Pierce County and PNWER with an advisory group that includes the U.S. Coast Guard, Washington State Fusion Center, Washington State Department of Transportation, Washington Ports Association, Port of Everett, and Everett Emergency Management.

Our analysis indicates that technology is a secondary strategy in overcoming challenges to community information sharing.

Difficulties Associated with the Complex ISE: In addition to looking at information sharing difficulties from the perspective of the role of technology, we also examined them from the perspective of the community's ability to navigate the complex ISE. We found difficulties associated with:

(a) Ambiguous pathways for information sharing

(b) Varying privacy and disclosure policies

(c) Uneven sharing practices

(a) Ambiguous pathways for information sharing - Increasing situational awareness is a key driver for information sharing across the community. This is not only true for incident response and management but also for day-to-day operations. Therefore, across the community, a day-to-day challenge that must be negotiated is determining who to inform and how and when to inform them. Individuals and organizations expend a tremendous amount of effort in this regard, and it is a core feature of day-to-day operational work. Ambiguity around what information is needed, how and when the information needs to be communicated, and with whom introduces overhead tasks required to resolve this ambiguity, which makes it difficult for community members to meet their operational goals. Eleven percent of information sharing difficulties described by interviewees were primarily due to ambiguity.

Ambiguity can appear in many areas: using equipment, structuring information sharing across partners, defining roles among partners, acting in accordance with privacy policies, knowing who to share what with when, knowing where to look for information, clarifying priorities, seeking funding, and interacting with oversight.

[There are] 8 lessors. Each have their own approved security plans with U.S. Coast Guard. Security plans aren't shared with the port or other lessors. This causes worry because the port doesn't know what the other security details will do in case of an event. It's hard to coordinate with lessors.

- APM Terminals security manager

Turnover was often mentioned as a case of not knowing who to contact, particularly by those who work with partners such as the USCG and USN where turnover is frequent. A lot of work goes into establishing relationship continuity among these information sharing partners as individuals rotate in and out of organizations.

Interviewees described some instances where a lack of guidance, framework, or structure hinders effective information flow. In some cases, organizational roles and responsibilities are not well-outlined. Some interviewees are concerned that without structure, they cannot process information rapidly and in turn respond appropriately.

When union workers discover a threat, their first priority is to call the U.S. Coast Guard. There is nothing in union workers' protocols that say they are supposed to call port security.

- A private security consultant

During an incident it may not be clear which partners need to by formally recognized. For example, one security consultant explained a situation in which the protocols of union workers were not written in a way that acknowledged other entities, in this case the port, that would be impacted by a threat discovered at a terminal.

(b) Varying privacy and disclosure policies - Policies and procedures guiding access and clearance fundamentally shape the Puget Sound maritime ISE. Interviewees report that access and clearance policies present challenges when those policies mistakenly distinguish "need to know" from "right to know." In such instances, community members may diverge from a mandated information sharing arrangement to ensure that trusted information partners are aware of the information they need to do their job.

As mentioned elsewhere, whether guided by internal policies or shaped by mandates and regulations, the privacy and disclosure policies that different organizations apply can vary considerably. While variation in policy is a feature of the ISE, interviewees stated that this challenge can be mitigated through joint planning and training, which helps collaborators become aware of the key elements that make information sharing successful — who needs to know the information, why they need to know it, when they need to know it, and how to share it with them.

A related challenge that stems from policies around information sharing is that in many instances information to be disclosed passes through a chain of permission that can curb the information flow and, on occasion, introduce errors.

(c) Uneven sharing practices - PSSSC members identified a few instances in which they were unable to obtain desired information. For example, tribal law enforcement expressed a desire to have access to law enforcement emergency communications so that they could contribute more effectively to enforcement actions that crossed tribal and non-tribal borders. A number of regional stakeholders complained of one-way information exchange with federal stakeholders and with other community members viewed as particularly closed in their communication channels/information sharing (*e.g.*, rail). Some of these uneven sharing practices are caused by the need for information security clearances. For example, a terminal employee explained, we "don't get threat information because of the classification. When the FBI presents at the AMSC meeting, because it is an open source meeting, it is always the same 'no credible threat.' Consequently, threat information is not given to the people doing security because of clearance level."

Similarly, a port security manager observed that while trying to maintain security, they get information up to a certain point, but then the flow of information stops because they "don't have the security clearance." This issue was also observed when the Seattle Emergency Management Center failed to get a threat assessment on a 2014 Seahawks sports victory celebration in downtown Seattle, which they believe was because they lacked sufficient security clearance.

Interviewees also frequently described the information sharing difficulties in terms of information content. This includes occasions of information overload or irrelevant content as well as concerns over the credibility, reliability, or timeliness of the content. Interviewees speculated on a possible cause for this; when many hands are involved in passing information among parties, errors are sometimes introduced.

Sometimes a call will go through multiple dispatchers before it gets to them. It's like a game of telephone and the original meaning can get lost. This gets better as relationships with other agencies gets better because they all start sharing a common language
- A county marine sheriff

The issue of unidirectional information flow, or instances where one partner takes information but gives little back in return, was a named difficulty in 13 instances. Most commonly the challenge concerned federal partners not filtering information back down, often for security reasons. A port security officer speaking of intelligence updates regarding possible eco-terrorist threats, said that this is "one of the most frustrating things. [The] Port is trying to maintain security, and we get information up to a certain point, but then the flow of information stops because we don't have the security clearance. . . it [information flow] is really one way."

While prevalent, this issue one-way information flow was not universal. Several interviewees described having good information sharing relationships with specific federal entities, and others acknowledged that although information flow sometimes feels "one-way," they understand the reasons for it. A WSP officer said, "Well, sometimes it feels like we are pushing the information up and it feels like we don't get anything back. But we just tell our people to push information up to the analysts at the fusion center because we don't know, it might be a piece of the larger puzzle." This officer also mentioned that they cannot always get information back from the WSFC for security reasons, but they just accept that that is how it is.

In some instances where interviewees described a unidirectional information flow, it was described as an obstacle to developing a common operational picture. For example, those who reported information about a suspicious activity up to federal entities but heard nothing back reported apprehension about not knowing how concerned they should be about the suspicious activity. Given that trust and relationships support much of the information sharing in the community, unidirectional information sharing could have the reverse effect. In at least one instance, an interviewee explicitly stated that organizations that do not communicate well are perceived as risky for collaboration.

Difficulties Associated With Modes of Communication: We analyzed reported information sharing difficulties in relation to the modes of communication associated with particular instances of information sharing, including (a) radio, (b) email, (c) social media, and (d) other modes.

(a) Radio - Radio interoperability — the ability to be on the same frequency as a partner organization — was among the most frequently mentioned technical difficulties in our data (8 instances). For example, radios used by the U.S. Coast Guard and by Seattle Police do not support communication among members of those organizations. This interoperability challenge was described as a "huge issue," "barrier," and "information gap."[20] One interviewee suggested linking interoperability across jurisdictional lines to funding for radio equipment. Two law enforcement officers expressed a desire to obtain encrypted radios.

A related, but distinct, challenge mentioned by a few interviewees is that digital radios do not work as expected, having different coverage patterns and usability issues than their analog predecessors. One interviewee described how narrowed coverage area has required considerable new investment in infrastructure. Reliability of radio receivers was mentioned twice. In one of the instances concerning reliability, the interviewee mentioned an information gap in knowing the reliability of equipment before purchase — a challenge he perceived as having high overhead.

Finally, one interviewee on the Olympic Peninsula complained about unevenness in coverage around the mountains, with all of the infrastructure along the coast. This interviewee attributed part of the difficulty to funding that only supports specific kinds of radio technology that do not work well given the Olympic Peninsula's geography.

Communication redundancy via phone was mentioned as a solution to radio issues.

A few years back we had a ranger shot and killed. I was the only one with a radio who could talk to the Coast Guard helicopter. Comm is a huge issue. NOTHING works in the Olympic Mountains. All the comm is on the coast. Once you get up here, you have zero.
- Tribal Fish and Wildlife Enforcement officer

(b) Email - While difficulties related to email were only mentioned by a handful of interviewees its place in the community as a primary channel can create a major obstacle to day-to-day work when it is not readily at hand. For example, a U.S. Coast Guard planner needs to be in frequent contact with collaborators outside of the .mil network, but policy and technical limitations associated with work email access is a "major barrier" in their day-to-day work.

Although the flexibility of email as a general-purpose communication tool is often a trait that provides greater usability, it was occasionally

Interviewer: *What irks you on a regular basis?*
Interviewee: *The key to this job is the informal connections, but because of the restrictions on mail and other restrictions you have to rebuild those connections. You cannot inherit your predecessor's email contacts to even know who to email first or what have you.*
- USCG Contingency planner

[20] Tribal Fish and Wildlife Enforcement officer

cited as a negative aspect. Email can be used to easily and quickly add collaborators, but one interviewee mentioned it is easy to inadvertently forget to include a collaborator. Email is employed for many different kinds of information sharing in the community, and one interviewee found that response to a call to action via email was much lower than when he reached out by phone. Another interviewee complained that he received too many emails, causing information overload. Finally, a fire chief expressed concern that email was too easily used to create policy. He did not want to put in writing something that was so easy to distribute widely via email.

(c) Social Media - For some community members, the adoption of social media is a challenge. Interviewees frequently mentioned their inability to use social media due to organizational policy. One federal interviewee described an instance where action on social media was needed in relation to an incident but policy and technical limitations prevented them from taking action. The interviewee reported that this limitation was circumvented by personnel who use their own personal communication devices and accounts when necessary. One community member reported a need for revised guidance on how to use social media.

(d) Other modes - Difficulties associated with phone use involved bandwidth capacity of cell networks during incidents and cell coverage area. Difficulties associated with face-to-face communication concerned lack of funding for travel or support for face-to-face meetings such as joint planning.

Community-Defined Coping Mechanisms for Difficulties of Information Sharing: In the course of describing information sharing challenges, interviewees often offered specific solutions for overcoming those challenges. To reduce the effect of difficulties on day-to-day information sharing, the community has put into practice a number of coping mechanisms.

Interviewees saw several solutions as effective means of increasing trust and shared understanding. Many individuals mentioned joint planning, joint training, and establishing and updating memoranda of understanding as keys to successful information sharing.

Face-to-face communication, which often occurred at these activities, was mentioned as a workaround or solution for a difficulty in several cases. For example, a U.S. Coast Guard planner explains how she uses face-to-face communication to circumvent challenges to email communication. "Because of the barriers associated with .mil, informal and face-to-face interactions are key to getting the job done."

The thing about the Coast Guard on sector level, so many different moving parts it's hard to know what is going on all the time. One way we try to alleviate (ambiguity) is have face-to-face meetings with captain and department heads.
- FEMA NIMS coordinator

Some community members remarked that they currently lack policies and guidelines for information sharing. Additionally, organizations work toward aligning situational awareness with each other. When community members identify the need for a policy change this does not necessarily mean a top-down mandate. While interviewees described the lack of guidance, policy, and procedures around information sharing, there is some evidence in their descriptions that suggest that, rather than a need for more policy, there may be a need to identify and cultivate specific expertise in information sharing among particular individuals.

Some interviewees reported making an effort to ensure that outgoing personnel introduce new people to their contacts. U.S. Coast Guard personnel report that current available technology works against efforts to maintain continuity contacts because there is no way for outgoing personnel to hand off their electronic contact lists and email contacts. Face-to-face interactions are also mentioned as a solution to ambiguity. A FEMA NIMS coordinator commented on the challenge retiring personnel pose to information sharing:

> Interviewer: "Is there any information that is hard to get, that you don't have access to?"
> Interviewee: "I think if you look at the results of every exercise, the things we have the most problems with - is command, control, and communications. We constantly have to make relationships. We constantly have to build bridges. We have the grey-hairing of Federal Government, right now. So you are losing a tremendous lot of knowledge. So we are going to have to work on building relationships. Because when it comes down to it, it is all about relationships."

Joint planning, training, exercises, and drills are viewed as effective means of aligning resources to establish new information sharing routines and reinforce old ones. Specific training on communication and information sharing was recommended.

5.7 *Aligning Information Technology with Mission and Workflow*

WHILE federal initiatives for improving operational effectiveness often focus on information technology, information systems that store, retrieve, and display information appear to play a relatively limited role in the overall information sharing environment.

Improving the utility of information systems demands a high degree of awareness about how the community operates. Few of the difficulties associated with information sharing can be addressed through purely technological solutions. As described earlier, particular information sharing challenges were attributable to a purely technological issue only 10% of the time. Among these are issues of bandwidth capacity, system errors, interoperability, data standardization, system and hardware functionality, user adoption, and the dependency on specialized but scarce personnel to operate equipment. As discussed, interoperability of radio and information systems were mentioned the most frequently and are viewed as serious issues by the community.

More frequently interviewees reported situations where there is a disconnect or misalignment between their workflow, information flow, and the supporting information system. Information systmes are resources that constrain operations, and they are not currently designed to constrain in the ways that people want to work. For example, USCG employees who investigate incidents must document them with photos but cannot readily incorporate those photos into their work process without resorting to their personal technology (*e. g.*, smart phones) and accounts.

> Frequently, information systems were viewed as causing problems because they did not align well with information flows and work flows.

The policy of acquiring and purchasing a one-size-fits-all technological solution prior to or without understanding the region-specific operational needs of PSSSC can lead to misalignments in the form of systems that add overhead and are not readily adopted. A new radar system in use by the U.S. Coast Guard demonstrated this issue. The technological specifications and need for types of radars vary dramatically from the east to west coast. The geography is different, and to upgrade systems that are purchased with a different requirements packet can be very expensive. Regional offices were required to find funding to upgrade systems so that they would operate in the regional environment. Federal sponsors often do not understand why additional funding is requested. If regional subject matter experts are consulted, it is usually an after-thought, and they are not engaged prior to the acquisition process for large technological solutions.

Several interviewees viewed policy and procedures to be the cause of misalignment between technology, information flow, and workflow. In six instances, interviewees attributed misalignments to the policy governing the use of information technology in their organizations. These policies did not always account for diversity and variation of work practices and information needs and resources across the community.

Other cross-cutting issues that appear in relation to mention of information systems include:

- Who can access a particular system
- Funding for deployment and implementation
- A need for more consideration of how a system can and should be used

The community indicated that an operational understanding of their work is necessary to produce acceptable solutions. For example, when asked why WebEOCs are not integrated, an interviewee from FEMA replied "They have no sense of what we do operationally and what we do in the field. But you can't develop a system to manage an incident if you don't understand how we manage an incident."

In several instances, interviewees indicated that inappropriate design processes inhibited the success of systems. For example, one interviewee expressed that no platform was available to support a common operational picture and that "no well-designed process for creating a SA-COP platform" is in place.

> Interviewees attributed difficulties to top-down design processes that ignored variations in needs, resources, and organizational culture.

One interviewee mentioned "forgotten" stakeholders who were left out of the design and provisioning process.

Systems are often added to try to incorporate and create better information sharing or SA-COP, but these systems do not replace or consolidate work; they are frequently inserted on top of existing systems. The number of systems is staggering. Design processes need to include a review of existing systems and possible redundancies.

5.7.1 *The Interplay between Day-to-Day and Incident-Focused Operations in Establishing Situational Awareness/Common Operation Picture (SA-COP)*

Situational awareness is a core concept of incident-driven information sharing. According to FEMA's National Response Network, situational awareness is "the ability to identify, process, and comprehend the critical information about an incident-knowing what is going on around you (requiring) continuous monitoring of relevant sources of information regarding incidents and developing hazards."[21] While FEMA's definition explicitly states that situational awareness

[21] DHS. (2008). National Response Network. Pg. 48.

concerns critical information about an incident, our analysis finds that the desire for situational awareness is a driver of day-to-day information sharing as well. Likewise, the processes that lead to situational awareness — identifying, processing, and comprehending critical information, as well as continuous monitoring of relevant sources — are established, maintained, and practiced outside of an incident. As one person involved in King County response explained:

> An initiative that we're now taking on is how situational awareness is developed at the city level and then shared at the county-regional level, and then how we develop a common operating picture with that. And it's the foundation of it. It's not a technological system. It's the: 'Okay, lets figure out where our gaps are' because we're not in a position to say, 'Hey, you have to use this system. You have to use this form. You have to do all these kinds of things. However you get us the information is how you get us the information. However, this is how we synthesize your information. This is how we might share it when we publish it out.' So that it's not just this laundry list of everything the cities send us. It's truly a synthesisation of what is happening within our region.

As this interviewee describes, the work of attaining greater situational awareness during an incident is improved by interagency interactions that take place among stakeholders in-between incidents. When situational awareness is developed, cultivated, and coordinated across several stakeholders this can lead to a common operating picture which the interviewee describes as "not a technological system."

Similarly, a 2012 FEMA training manual defines a common operating picture in more technological terms as "a continuously updated overview of an incident compiled throughout an incident's life cycle from data shared between integrated systems for communication, information management, and intelligence and information sharing."[22] This definition suggests a technological solution for constructing an operational picture, but as our research has revealed, the system is, in essence, the community, and by extension the integration takes place during activities that focus on identifying the essential elements of information that support decision making. Those we interviewed did not rely solely on any technological system to comprehend an event. Nor did they turn to only one information system to understand an event, but rather reported using multiple modes of communication. These alternative channels, sometimes employed with tools intended to aid a common operational picture, suggest that the need to work with others in a collaborative fashion to establish a ground truth is integral to developing a common operational picture, and that the community is continually building situational awareness and developing a common operational picture to suit their unique

[22] FEMA NRF Resource Center. (2012). L0948 Student Manual - Situational Awareness and Common Operating Picture Student Manual L0948

operational needs.

Understanding the operational environment and the regional use of information is the foundation of an SA-COP, which is often viewed as incident-focused and technology dependent.

Day-to-day situational awareness is fluid, dynamic, and continuous. It expands beyond what is needed to achieve SA during an event, because during day-to-day operations the focus of the work is not tied to one event but the overall organizational mission, both long-term and short term. Incidents often focus on the events that are 24, 48 and 72 hours out, while day-to-day operations focus on present and future cycles that may have a much longer-term strategic life.

6 Regional Systems and Standards

6.1 *Summary*

As an adjunct to our Phase 1 effort, we looked into the IT systems used by the agencies interviewed with a focus on how systems used tagging, achieved identity management, and whether the systems used any sort of data standards. We gathered information about the systems from IT professionals at the organizations and from the users of the systems. Given the goal of identifying data standards, identity management techniques, and use of tagging, we focused on proprietary systems or enterprise software used by entities for specific functional purposes in support of day-to-day activities. This excluded radio communications, and sensor systems. Overall the PSSSC showed very little interest in, or even awareness of, the use of data standards, metatagging, or national exchange models.

6.2 *Methodology*

Initially we planned to conduct IT interviews at the same time as the general Phase 1 interviews were being conducted. We quickly realized, however, that many of the agencies we were interviewing did not have in-house IT people. (This itself was informative.) Our revised plan was two-fold. First, the analyst used information gleaned from several formal interviews to understand how the users perceived the systems in place; second, we attempted to get contact info for IT personnel during the general interviews. Many of the follow-on IT-specific interviews were conducted with IT helpdesk personnel who could neither speak to the technical aspects of how the systems worked nor whether they used standards. We were able to gather some of the missing information from Internet searches.

6.3 Results

Through our interviews and Internet searches we identified a total of 59 systems in use by the regional safety and security community. Of those 59, 32 are federal and 27 are local (see Appendix F for details on the local systems; see the MOISA HSIN site for the entire table).

All of the entities interviewed reported email as being the most heavily used system for information sharing, with phones or in-person meetings being the other most heavily used modes. In all cases, enterprise IT systems were used only when email or phone could not get the job done faster or, more often, when they were required to use IT systems.

We were instructed to focus on the non-federal systems. Of the 27 non-federal systems we identified, seven used some form of tagging, and of those, only one, *Spillman*, adhered to a standard set of tags. During the interviews, most people did not understand the question about the use of tagging in systems. Several interviewees told us that they would not use tagging because that would require storing more data than they would like. We were also told that because Washington is a Home Rule state, they try to store as little data as possible in systems to avoid having to release sensitive data to the public.

The systems we found that got the most use were systems that had a specific purpose, like *Common Operating Response Environment* (CORE) for radiation/nuclear detection, or mass messaging systems like *NorthWest Warning, Alert, and Response Network* (NW WARN). The one exception to this was the *Spillman* system.

Spillman is a commercial dispatch system. Several counties acquired licenses for *Spillman* across the state using Port Security Grant Program (PSGP) money. The software was modified to fit the needs of each entity, and was then upgraded using more PSGP money to link the entities together, allowing them to share available information and resources (*e.g.*, location of boats and fire trucks), allow dispatch systems to talk to each other, and for the connected entities to message each other. *Spillman* was identified by its users as one of the most successful systems in the region. We asked one entity to compare *Spillman* to *Maritime Common Operating Picture* (MCOP), a project with overlapping capabilities being developed in Seattle also funded by PSGP money. They responded that MCOP will be very similar, but that they were not sure why *Spillman*, a system already developed and in place in parts of Washington, was not adopted instead of building a whole new system.

Another heavily used system we found is CORE, a system maintained by the Pacific Northwest National Laboratory and used during radiation/nuclear events. It allows for situational awareness and analysis. The DNDO Joint Analysis Center (JAC) has a similar system, JACIIS, for land-based nuclear threats. CORE has an API that would allow for JACIIS to ingest data from CORE; however, JACIIS does not currently do this.

We attended several presentations and demonstrations regarding the ongoing development and implementation of MCOP. MCOP is a set of eight applications intended to provide situational awareness and allow for information sharing. Several of the applications, such as *ViewPointe* and *CommandBridge*, are already in use by different entities in the Seattle area. MCOP would not replace these systems but would act as a portal to log into all eight. It would also allow users access to the other seven systems they did not already use. At the time of our interviews, MCOP had not been rolled out, but it seemed to be met with skepticism by users. A common sentiment, as expressed by one potential user was, "This looks interesting, but it is just one more system for me to keep track of."

Another system in development that we learned of that allows some integration with other systems is *FirstToSee*. *FirstToSee* uses social media to add information to maps during disasters or events. *FirstToSee* has an API that allows it to share data with other applications like WebEOC. It uses tags, but they are not standardized. *FirstToSee* is being developed with PSGP funding.

A majority of the agencies we interviewed used DHS's SharePoint-based system HSIN. However, only three entities upload information to HSIN; all others only download information.

None of the systems we identified are able to talk to one another with the few exceptions noted above. The few cases where we saw systems in place that allowed different entities to share information were proprietary systems installed in a region that did not talk to other proprietary systems, *e.g.*, MCOP and *Spillman*.

Many of the larger systems mentioned above (MCOP, *Spillman*, CORE, *FirstToSee*, *CommandBridge*, *ViewPointe*) serve a similar purpose for their users; however, they do not share a common set of data standards and have no way to communicate with each other.

The entities interviewed fell into three categories of system use:

Group 1. Entities that had many systems they had to keep track of and use. These were mainly federal entities.

Group 2. Entities that had a few (2-3) main systems they used. These were mainly larger local entities.

Group 3. Entities that did not rely on information systems on a day-to-day basis. These were mainly smaller local entities.

Group 1's main complaint was that there were too many systems to keep track of and use, and because of this, the systems do not get used to their fullest potential and the users fall back to email, phone, and face-to-face meetings when possible. The members of group 2 generally seemed to be satisfied with the systems they used, except when it prevented them from working with other entities that did not have access to those systems. Group 3 generally did not feel the need to adopt a system to help with day-to-day work. This group did not have in-house IT, and the entities felt that phone and email were all they needed to get their work done. We did hear some complaints from entities that fall under group 3 that they sometimes got left out during large events. If the small entities in group 3 had the support to be part of the larger systems, it might help build relationships and encourage more interoperability.

6.4 Conclusion

The few local entities that are using enterprise systems seem to be doing so with some success internally but not so much for interagency information sharing. The success with *Spillman* users indicates that if entities could adopt common systems that allowed for greater interoperability, it would enhance their coordination.

Local entities felt that systems need to be customized for their individual use but should also allow entities across the region to talk to each other. This could be done using a single vendor, or by requiring individual vendors to adhere to a set of standards that would allow the applications to tie into each other. Another alternative being explored at the federal level is an Ozone Widget Framework (OWF)[1] that would allow entities to connect and manage their individual web applications in a single operating environment. Implemented with community buy-in, this could help reduce the number of systems that larger Federal agencies have to keep track of and could encourage interagency operability across the region.

[1] http://www.ozoneplatform.org/

7 Phase 2: Interagency Dependencies and Use-Cases

7.1 *Summary*

In this section, we present our process for using Phase 1 interview data to down-select to a single use-case for analysis in Phase 3. The primary contribution of this phase is the selection of a Phase 3 use case, and the secondary contribution is a survey of the types of business processes that are prevalent in the community and the degree to which they require interagency collaboration as reported by interviewees.

The findings from Phase 1 presented in Section 5 gave us a broad understanding of the socio-technical system that supports maritime safety and security on a day-to-day basis, and in Phase 3 we present our analysis of a deep dive into a particular aspect of this system. Phase 2 was a necessary, interim step required to determine the scope of the model presented in Phase 3 and is the transition from the Phase 1 broad analysis to the Phase 3 deep dive.

Here we include a brief discussion of scoping modeling projects including the use-case and scenario concepts in systems engineering, how the exploratory approach to the modeling methodology that we used in Phase 3 necessitated this methodological step, and how we developed the use-case selection criteria and operationalized it to analyze interagency interdependencies. We conclude by discussing the results of this analysis and additional considerations that led to our final use-case selection.

7.2 *Objectives*

The objectives of phase 2 were to:

- Document and analyze interagency dependencies
- Identify and characterize use-cases prevalent in community

- Develop criteria to identify a use-case involving information sharing for deeper analysis
- Use these criteria to down-select from use-cases that were documented in Phase 1 interviews to the scope of a single use-case for Phase 3 analysis

7.3 Methodology

To determine the scope of the Phase 3 effort, we developed criteria for selecting a use-case from a subset of use-cases that emerged from Phase 1 interviews. We encoded these variables into Phase 1 text data using a software tool[1] and accompanying relational database. We then queried and analyzed these data to score possible use-cases along our selection criteria. Based on these scores, we selected the best possible candidate use-case.

7.3.1 Background

Determining the scope of a model is a critical and often challenging aspect of any modeling project. Although discussion of the Phase 3 methodology is presented in Section 8.4, understanding the importance of Phase 2 in scoping the Phase 3 model requires a brief introduction to the Phase 3 methodology. Our model-based systems engineering approach is flexible and can be applied in multiple ways to achieve different analytical products. These applications and their products fall into three categories:

Application 1. Exploratory analysis: Product is an understanding of the flow of process-critical information and where and how information is used.

Application 2. Directed, problem-driven analysis: Product is the evaluation of candidate process change(s) and measures of predicted impact.

Application 3. Directed, design-driven analysis: Product is the design and evaluation of candidate process change(s) and measures of predicted impact.

For the second and third applications, the scope of the model is defined by the scope of the candidate process change. We conducted an exploratory analysis (Application 1) since we did not assume that there were any existing problems. Our analysis did not have a predetermined scope, but rather requires a principled process for

[1] Dedoose. http://www.dedoose.com/

identifying the boundaries of what will be included in the model and what will be left out. In the following section, we describe how we used the Phase 1 data to determine the scope of our Phase 3 exploratory analysis.

7.3.2 *Conceptual Framework*

Use-cases and scenarios are well-known concepts in systems engineering and design. The use-case and scenario constructs help us scope modeling projects and provide us with guidelines for how to break large complex systems that might otherwise be intractable into manageable sub-systems for analysis.[2]

A use-case is a prose or graphical description of a system's behavior when interacting with the outside world. A use-case is comprised of scenarios: "A scenario is a sequence of actions that illustrates behavior"[3] and appears within a use case model as a single thread or pathway through the use-case.[4] In this sense, a use-case is a collection of scenarios that are possible within the system.

The purpose of a model of a use-case is to provide a view of possible interactions (including information exchange) among people and objects towards a particular goal within a specific context of work. By developing use-case models and scenarios, we can understand system requirements. As domain expert knowledge is often tacit, lists of system requirements, even when gathered from the system users, are often inaccurate or incomplete.[5] Unlike typical methods of requirements gathering, use-cases and scenarios are part of an extended process of requirements development in collaboration with system users. Use-case models have a higher probability of supporting the design of a system that satisfies requirements because they describe the system's functions as derived from an understanding of different types of users, their different types of interactions with the system, and the environment or context of use.

Given the vast breadth of the use-cases and scenarios described by interviewees during Phase 1, deciding on a single use-case for our deep dive in Phase 3 was an important methodological step.

7.3.3 *Development of Use-Case Selection Criteria*

In collaboration with our sponsors, we first established criteria that our use-case must meet in order to enable Phase 3 analysis. Namely, that it involve (1) information sharing where there was some difficulty sharing or obtaining information and (2) a diverse

[2] Rosson, M.B. and Carroll, J.M. (2009). Scenario Based Design. In *Jacko, J. & Sears, A. (Eds.), The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications.* Lawrence Erlbaum Associates, 2002, pp. 1032-1050.

[3] Rosson, M.B. and Carroll, J.M. (2009).

[4] Sutcliffe, A. (2003). Scenario-based Requirements Engineering. *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International.* pg. 320-329.

[5] Carroll, J.M., Rosson, M.B., Chin, G. and Koenemann, J.R. (1998). Requirements Development in Scenario-Based Design, *Software Engineering, IEEE Transactions on,* vol 24. pg. 1156-1170.

group of stakeholders where (3) the connection to security operations was medium or high. Additionally, the use-case had to be (4) an example of inter-agency interdependency, (5) of interest to the broader community, and (6) of interest to our sponsors. Finally, for practical reasons, (7) the stakeholders involved in the use-case had to be available to participate in Phase 3 interviews and observations.

7.3.4 *Data Encoding for Use-Case Selection Variables*

WE operationalized criteria 1-3 as codes that we used to analyze a representative sample of Phase 1 text data. Codes are applied to excerpts of the data that are evidence to the concept that the code represents.[6] Using the software tool, Dedoose, three researchers coded a representative sample of the data using this top-down coding schema. The researchers coded the data independently and then conducted debriefing sessions to review discrepancies and achieve consensus on the final code applications.

7.4 *Data Analysis*

WE first coded for all mentions of security in the data. Based on the frequency and way in which references to security were documented, we assigned a numeric score (1 = none; 2 = some; 3 = high) to each interview to indicate the magnitude of the interviewee and/or their organization's role in security as documented in the interview. As we were only interested in scenarios that were related to security, interviews with a score of 1 were excluded from subsequent analysis.

Within each of the interviews with a "role of security" score of 2 or 3, we identified all excerpts that referred to work scenarios involving information sharing. For each of these excerpts, we assigned a numeric code to represent the level of difficulty of information sharing evidenced in the text (1 = not at all difficult; 2 = somewhat difficult; 3 = difficult). We also counted the number of entities involved in the scenario, as reported by the interviewee.

We then identified the most prevalent scenario types by grouping all information sharing excerpts into emergent use-case categories. These categories were (in order of prevalence):

1. coordinated dispatch
2. securely moving cargo
3. coordinating international vessel traffic

[6] Saldaña, J. (2012). The Coding Manual for Qualitative Researchers (No 14). Sage Publications, Inc.

4. managing maritime casualties
5. addressing suspicious activity (non-port)
6. managing public/special events
7. maintaining general port security
8. maintaining ferry security
9. navigating the role of tribal security

Within each of these categories, we calculated the mean score for "role of security" across all of the interviews in which scenarios that would fall under these types of use-cases appeared. As a measure of interdependency and use-case complexity, we counted the total number of unique entities involved in these types of scenarios as reported by interviewees. Finally, we calculated the mean difficulty score for all information sharing excerpts for every interview in each category.

The research team and the sponsor team reviewed the output of the above analysis and then scored each use-case category along criteria 4-7.

Table 7.1: The use-case selection matrix for Phase 2.

			Use-Case Selection Criteria							
			1	2	3	4	5	6	7	
	Areas of overlap	Use-case candidates	Role of security (mean)* (*Mean score for interviews in which reference appears*)	Number of unique organizations mentioned as being involved	Effort to obtain/share information (*Mean for all excerpts that are evidence to scenarios within the use-case†*)	Degree of dependency‡	Degree of interest to broader community‡	Degree of interest to sponsors‡	Availability and involvement of key informants‡	Total
A	F	Coordinated Dispatch	2.5	10	1.8	3	1	2	2	22.3
B	H,C	Movement of Cargo	3	16	1.83	3	1	3	2	29.83
B1	H,C	Oil arriving to port by train	3	2	1	2	1	1	1	11
B2	H,C	Exceptional cargo arriving by truck	3	2	1	2	2	1	1	12
C	B	International coordination of vessel traffic	2.5	4	2	3	1	2	2	16.5
D	E,G	Waterway safety processes	2.5	13	1.38	3	1	3	3	26.88
E	D,G	Manage maritime casualties	2	4	1.4	2	1	3	3	16.4
F	A	Address suspicious activity (non-port)	2.29	8	1.52	2	1	1	3	18.81
G	D,E	Manage public/special event	2.8	7	1.57	2	2	2	2	19.37
H	B	Maintain port security	3	7	2.38	3	1	3	3	22.38
I	-	Maintain ferry security	2.5	2	-	2	1	2	2	11.5
J	F	Tribal security role	2	8	1.2	1	2	2	2	18.2

*2 = some, 3 = a lot; interviews with a score of 1 were excluded.

†1 = not difficult, 2 = somewhat difficult, 3 = difficult.

‡1 = low, 2 = medium; 3 = high.

7.5 Results

Results of Phase 2 analysis are presented in Table 7.1. The scenario categories are listed in order of the prevalence of the scenarios that fall under each category. Many of the use-case categories intersect or overlap, and column 2 lists overlapping or intersecting use-case categories.

The category of *securely moving cargo* met all of our criteria and had the overall highest scores. We were concerned about the availability of some key informants for the cargo movement use case, but after considering other high-scoring categories, we determined that cargo movement would be the best option. For example, we considered the category *maintaining general port security*, which had the second highest score, included more scenarios where sharing/obtaining information was difficult, and scored better than *securely moving cargo* in the availability of key informants. However, we determined that the scope of port security is too general and was not sufficiently scoped to be a first choice proof-of-concept. *Securely moving cargo* was more prevalent and more tractable than *maintaining general port security*; we selected the cargo movement use-case as the subject of Phase 3, despite potential difficulties accessing informants.

7.6 Discussion

The Phase 1 data proved invaluable for scoping a use-case of interest for deeper analysis through modeling. Our values for each criteria (*e.g.*, criteria 3 - the number of other entities involved) are only as accurate as the numbers reported in the interview and are not exhaustive.

8 Phase 3: Modeling Containerized Cargo Operations Use-Case

8.1 Motivation

> *We fail more often because we solve the wrong problem than because we get the wrong solution to the right problem.*
> - Russell Ackoff

FEDERAL interventions in the maritime community may miss the mark or introduce unintended consequences when the designers fail to understand what the problem is. One approach to obtaining the necessary understanding is to directly ask the community what they view the problem to be. This approach, however, generates a list of pain points, *i.e.*, symptoms of the problem, and fails to identify the problem itself. Another approach, one that advances both the designers' and the community's mutual understanding of the problem, is needed to develop interventions that will truly benefit the stakeholders. This later approach requires mechanisms for increased user input and ownership so that the community becomes an equal partner in the design, development, and implementation of interventions.

In this section, we present how MOISA executes this community-centered approach for one specific use-case. The outcome of the approach is a strong understanding of the work completed and the information used in the use-case. This is accomplished through the creation — by the research team and the community members — of a model of the use-case. The benefits of a model-based approach are discussed in this section, but a key point to remember about models is that they are built from a particular viewpoint. Frequently (and perhaps this is the reason systems fail to catch on in the community) models are built from the federal or developer viewpoint rather than the community or workflow viewpoint. The methodology presented here integrates both viewpoints to achieve solutions that satisfy all stakeholders. Phase 3 demonstrates a methodology that allows the community to mature its understanding of its work processes and information needs, communicate and build upon that understanding with external designers, and drive the design of interventions intended to improve its operations.

The results and disussion presented in this section refer to the specific use-case identified in Phase 2 and demonstrate the power of the approach, which can be applied to any desired use-case. The outcome of the model — identifying who exchanges what information, with whom, why the information is necessary, and how the information exchange must occur[1] — is the necessary information to invest in systems and programs that will in reality meet the maritime community's information sharing needs.

8.2 Summary

Phase 3, in terms of person hours, comprised about 15% of the overall MOISA project effort. Phase 3 consisted of the development of a detailed model of cargo operations (the central business operation of a terminal), the corresponding security information flow, and the manner in which the use of current information resources constrain operations. The deliverable of Phase 3 is a graphical model[2] developed using a model-based systems engineering (MBSE) approach and implemented using an extension of the Business Process Modeling Notation (BPMN) standard. Model development is an iterative activity conducted with the practitioner community that produces a detailed agreement on how work is conducted and information is used in support of that work. In addition, the model generates an information dictionary of security information (Appendix H) as it is used within the workflow of cargo operations. The MBSE approach of generating the information dictionary aligns with important federal efforts to capture essential information exchange requirements. The technique connects work behavior to information flow, and it can be applied to analyze trade-offs between better information resources and more physical resources and to identify where and how future systems and programs will impact current operations.

8.3 Objectives

Phase 3 focuses on demonstrating our approach to understanding information sharing in the community with the community members acting as equal partners. One goal is to demonstrate the added

[1] "Information exchanges express the relationship across the three basic architecture data elements of an operational architecture (operational activities, operational nodes, and information flow) with a focus on the specific aspects of the information flow and the information content." DOD. (2007). DOD Architecture Framework, Version 1.5, Volume 2: Product Description.

[2] The model is available on the MOISA HSIN site.

value of using a model-based systems engineering approach to meet our objectives. The added value of increased accuracy, generality, scalability, and cost-effectiveness is derived from the skills and labor required in building the model, the cooperation of and time donated by professionals involved in cargo operations, the scalability of the approach, the generality of the findings, the analytical power of computational models, and the potential for their re-use. In order to demonstrate how our methodology achieves this goal, we carry out the approach for one use-case: cargo operations at a container terminal. The use-case specific objectives are then to identify security information resources and the policies for using them that impact cargo operations workflows. The use-case objectives are to understand and model:

- The use and generation of security information in support of containerized cargo unloading operations at a marine terminal.
- Security as a service in support of those operations.

8.4 Methodology

In the following section, we describe our model-based systems engineering approach to understanding the cargo operations use-case and the related use of security information.[3]

8.4.1 Context

The scenario that was selected during the Phase 2 analysis was cargo operations at a U.S. port of entry. These operations are critical to our overall national security and a component of the DHS strategic priority to "minimize the disruption to and facilitate the safe and secure inbound and outbound legal flows of people and goods."[4] A 2013 economic impact assessment of U.S. west coast ports found that ILWU[5] terminals support 9.2 million workers who received $383.1 billion in wages and salaries. The cargo transiting the west coast ILWU terminals[6] generated $2.1 trillion, which represents 12.5% of the U.S. GDP (2014).[7] The valuable role that seaports play in our economy makes them a target. For example, the successful nuclear terrorist attack on a U.S. seaport[8] has been estimated to result in "disruption of U.S. trade valued at $100-200 billion, property damage of $50-500 billion, and 50,000-1,000,000 lives."[9]

The objective of the seaport system is to transfer goods and passengers between maritime and inland modes of transportation

[3] For additional detail, see Butler, K., Bahrami, A., Schroder, K., Braxton, M., Lyon, L., and Haselkorn, M. (Forthcoming 2014). Advances in Worflow Modeling: The Modeling & Analysis Toolsuite for Healthcare (MATH). In *University of Washington Final Report to SHARP-C*. Available at https://depts.washington.edu/ahrqserv/docs/MATH_method_for_MOISA.pdf

[4] 2014 Quadrennial Homeland Security Review, DHS

[5] International Longshore and Warehouse Union

[6] The west coast ports account for 43.5% of U.S. imported containerized cargo and 40% of exported containerized cargo.

[7] Martin Associates. (2014). Economic Impact and Competitiveness of the West Coast Ports and Factors that Could Threaten Growth.

[8] Using data from the ports of New York, Washington, D.C., and Boston

[9] Abt Associates. (2003). The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability. pg. 3

quickly, safely, and cost-effectively. The physical elements of the system include container terminals, cranes, intermodal containers, vessels, trucks, railways, employees, etc. There are numerous FSLTIPP stakeholders in the port system, including but not limited to, federal agencies, *e.g.*, CBP, USCG; non-governmental organizations, *e.g.*, pilots associations, towage; state and local authorities, *e.g.*, fire, police; labor unions, *e.g.*, ILWU; port authorities, *e.g.*, Port of Seattle; customers, *e.g.*, importers; and industrial partners.

8.4.2 Conceptual Framework

The Institute of Electrical and Electronics Engineers (IEEE) defines a model as "an approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system."[10] We used a model-based systems engineering (MBSE) approach, in contrast to a document-based (DBSE) systems engineering approach. In the DBSE approach, documents are the main product of the analysis; the requirements document defines the functions of the system. In MBSE, the main product is a model of the system; the purpose of the model is to formally elicit systems requirements from users.[11]

The resulting model serves as the descriptive scenario, *i.e.*, it describes the current, or as-is, process and captures both satisfactory and unsatisfactory elements. Identifying the descriptive scenario is consistent with work-centered design.[12] In this approach, the analyst develops system requirements via observations and walkthroughs of the work process and the information that is required to perform each task. Because these walkthroughs are led by the stakeholders who actually perform the work, the model connects system requirements with user behavior, which in turn, supports the design of system interventions that align with the actual rather than hypothetical workflow.

User-stated requirements can sometimes contradict observed work patterns. For example, an earlier study reported that while Puget Sound stakeholders stated that they desired a "one number, one guy" approach to maritime domain awareness; in reality, their work patterns show a preference for private internal communication.[13] The point of developing requirements is not to produce a document, but rather to understand the business process at hand and what is necessary for its successful completion. Meeting the stated requirements does not guarantee that the system meets the stakeholders' needs, but by deriving requirements from an explicit understanding of

[10] IEEE. (1990). Standard Glossary of Software Engineering Terminology. IEEE Standard 610.12-1990.

[11] Harvey, D., Waite, M., Logan, P. and Liddy, T. (2012). Document the Model, Don't Model the Document. 6th Asia Pacific Conference on Systems Engineering, Brisbane, Australia, 30 April - 2 May, 2012.

[12] K. A. Butler, J. Zhang, C. Esposito, A. Bahrami, R. Hebron, and D. Kieras, (2007). Work-Centered Design: A Case Study of a Mixed-Initiative Scheduler. *CHI-Conference*, Vol. 1, pp. 747-756.

[13] Salem, A., Walsh, W., & Englehorn, L. Maritime Information Sharing Taskforce. Naval Postgraduate School (2009). Industry and Public Sector Cooperation for Information Sharing: Ports of the Puget Sound.

stakeholders' workflow, we dramatically increase the odds that it will.

The system model is dynamic and can be viewed in many ways (*e.g.*, data and information view, operational view, stakeholder relationship view). The system model serves as

> a strategic information asset that describes the current and/or desired relationships between an organization's business, mission, and management process. [It] defines a strategy for managing change, along with transitional processes needed to evolve the state of a business. [It] defines the principles and goals and sets direction on issues such as the promotion of interoperability, intra- and inter-agency information sharing, and improved processes.[14]

8.4.3 *Methods*

Our approach is iterative and comprises three stages (Figure 8.1):

1. Knowledge acquisition in which we collected observational and interview data from subject matter experts, analyzed work artifacts and national data standards, and critically reviewed literature and government reports.
2. Modeling in which we encoded this information into a graphical language that produces an interactive model of the workflow and information flow in support of cargo operations.
3. Analysis in which we analyzed this model to identify information gaps and inconsistencies.

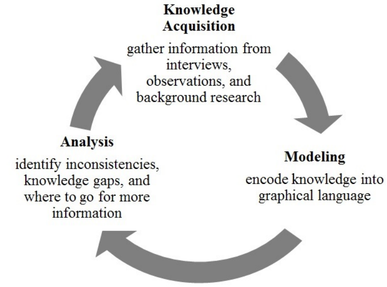
Knowledge Acquisition
gather information from interviews, observations, and background research
Modeling
encode knowledge into graphical language
Analysis
identify inconsistencies, knowledge gaps, and where to go for more information

Figure 8.1: Three stages of the iterative modeling process: knowledge acquisition, modeling, and analysis.

Model Subject: The study setting was the APM Terminal,[15] located at the Port of Tacoma which handles domestic and limited international cargo vessels and has scheduled, opportunity, and preferred[16] business.

Participants: Using snowball sampling, we interviewed six individuals in job roles critical to the scenario under study:

- terminal operations and security managers (2 individuals),
- USCG inspectors (2 individuals),
- a trucking company representative (1 individual),
- a U.S. Army logistician specializing in offloading military cargo (1 individual)
- ocean carrier operations, business process, IT, and customer service employees (4 individuals)

[14] Department of Defense. (2010). The DoDAF Architecture Framework Version 2.02.

[15] Referred to in this report as APM Tacoma or simply APM.

[16] Preferred business refers to the Port of Tacoma's preferred use of APM's berths. Preferential berths are a provision of APM Terminals contract with the Port of Tacoma.

- a freight forwarder (1 individual)

We also spoke with 3 CBP inspectors who were present Port of Tacoma event for USTRANSCOM in Fall 2014. This interaction was not an interview, but we did speak with them regarding the port-related topics addressed at the event.

Knowledge Acquisition: The knowledge inputs into the model are interviews with subject matter experts and source documents including work artifacts, literature, and government reports. We conducted a total of 12 hours of in-person interviews with subject matter experts and an additional 35 hours of supplementary data collection (source documents), modeling, and analysis.

We began by interviewing a terminal security officer who also provided us with sample work artifacts, *e.g.*, computer print outs of planning documents, manifests, and email communication. The focus of the interviews was on understanding the interviewee's work processes and associated information, where and how they get the information, and what they do with it. Knowledge elicited during this interview was then encoded into a high-level workflow model. Using the model as a guide, we identified knowledge gaps, individuals we needed to talk to for missing information, and what questions to ask next. Basing our interview questions on the draft model resulted in very focused and detailed interviews that elicited insights critical to the workflow. Supplementary information was gathered from publicly available sources such as the CBP website and the United Nations' Rules for Electronic Data Interchange for Administration, Commerce, and Transport.

Following this methodology, the knowledge acquisition process is iterative, and we went through several cycles before achieving a complete picture of the tasks that comprise the scope of the selected workflow and the supporting flow of information.

Modeling: An essential element of MBSE is a common language that is clear and unambiguous. The declared language in the cargo operations model is an extension of the Business Process Model and Notation (BMPN). The BPMN extension, MATH,[17] enables the analyst to capture information flow in support of the BPMN workflow.

The initial scope of the model was determined by our analysis in Phase 2. The depth of the model was determined by the level of granularity at which we could observe information flow and information dependencies. The integration of work and information flow is key to understanding how security information is used and generated in the process of transporting containers from a vessel,

[17] For additional detail, see Butler, K., Bahrami, A., Schroder, K., Braxton, M., Lyon, L., and Haselkorn, M. (Forthcoming 2014). Advances in Worflow Modeling: The Modeling & Analysis Toolsuite for Healthcare (MATH). In *University of Washington Final Report to SHARP-C*. Available at https://depts.washington.edu/ahrqserv/docs/MATH_method_for_MOISA.pdf

through the marine terminal, and finally to the inland transportation network via truck. Figures 8.2 and 8.3 illustrate the graphical language of the model and show the top-level of the model and the process of intermodal transportation at the container terminal, which is itself a subprocess of cargo operations.

Analysis: Through a critical review of the as-is model of information flow that enables the cargo movement workflow, we uncovered information dependencies among different operational divisions at the terminal (*e.g.*, security and operations) as well as between the terminal and outside agencies including the USCG, CBP, trucking companies, and ocean transport. We then researched policies and initiatives that constrain information sharing in the as-is workflow. In addition, we identified pending initiatives with the potential of impacting current operations and information sharing relationships.

8.5 Results

This section describes the scope of the model, an example path through the model, and security measures taken regarding cargo operations and the information required to carry out those measures.

8.5.1 Model Scope

The terminal was the initial starting point from which the model was built. APM Tacoma handles container and break-bulk cargo; only containerized cargo is considered in the model. As there is no on-dock rail, all intermodal transportation in and out of the terminal is via truck. The model aims to follow one container through the entire process of cargo operations.

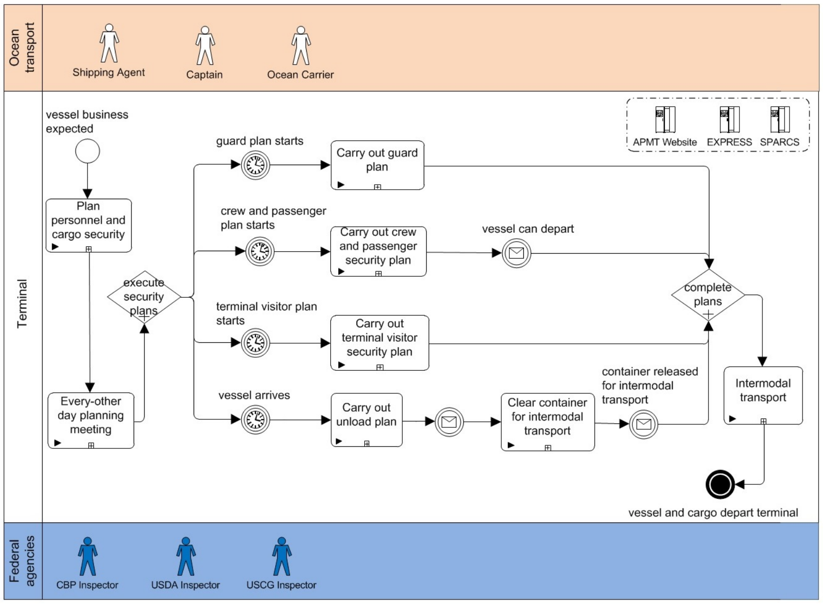
Ocean transport
Shipping Agent
Captain
Ocean Carrier
Terminal
vessel business expected
Plan personnel and cargo security
execute security plans
Every-other day planning meeting
guard plan starts
Carry out guard plan
crew and passenger plan starts
Carry out crew and passenger security plan
vessel can depart
terminal visitor plan starts
Carry out terminal visitor security plan
vessel arrives
Carry out unload plan
Clear container for intermodal transport
container released for intermodal transport
complete plans
Intermodal transport
APMT Website
EXPRESS
SPARCS
vessel and cargo depart terminal
Federal agencies
CBP Inspector
USDA Inspector
USCG Inspector

Figure 8.2: The top-level of the model shows the major tasks involved in container terminal operations. Lower-levels of the model show further detail for these tasks.

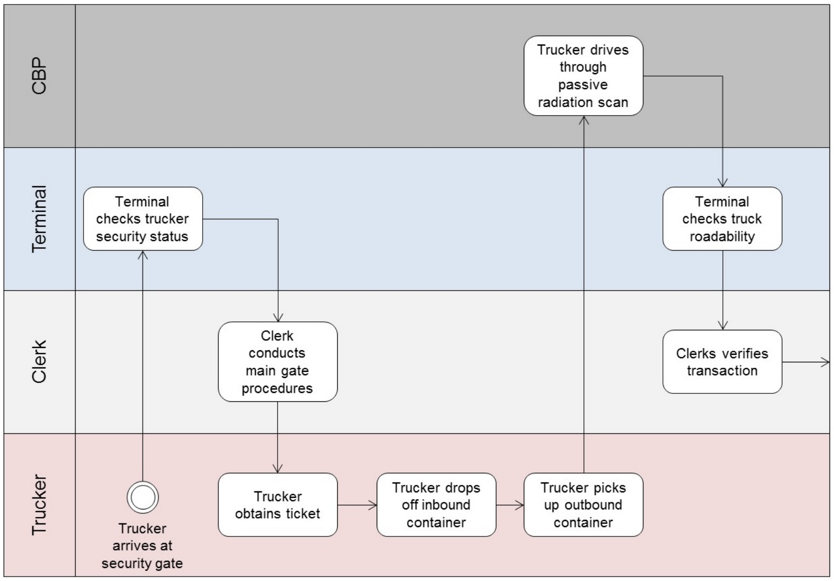
CBP
Terminal
Clerk
Trucker
Trucker drives through passive radiation scan
Terminal checks trucker security status
Terminal checks truck roadability
Clerk conducts main gate procedures
Clerks verifies transaction
Trucker arrives at security gate
Trucker obtains ticket
Trucker drops off inbound container
Trucker picks up outbound container

Figure 8.3: This level of the model shows the task involved in the intermodal transport portion of the overall model.

The information used throughout the model is collected into an information dictionary. This information dictionary itemizes all information that is essential to the terminal's workflow and in which tasks it is used. To illustrate information usage in the model, the next section will guide the reader through a representative path in the model and show the relevant portions of the information dictionary (Appendix H).

8.5.2 *Example Path in Model*

Figure 8.2 shows the top-level of the model and illustrates the model's terminal-centric nature. The white swimlane contains the terminal's tasks, while the orange and blue swimlanes contain the information resources of the ocean carrier and federal agencies, respectively, involved in maritime trade. Lower-levels of the model show higher levels of detail and contain information flows.

As the model shows, there are two aspect of security around cargo operations: (1) the local physical security of the terminal's perimeter and the people within it and (2) the terminal's role in external interactions with the larger supply chain security. The workflow depicted in the model begins when a vessel is expected to call at the terminal. This triggers the terminal's security manager to assess the perimeter and personnel security needs. Perimeter security involves manning the terminal gates and roving the premises. Personnel security pertains to authorizing[18] and enabling[19] the crew, passengers, visitors, and vendors to enter and exit the terminal.

Task: Review personnel information
Information Input:
From the Captain's email: crew manifest, passenger manifest, visitor list, shuttle request;
From the Port Engineer's email: vendor list
Task: Review vessel schedule
Information Input:
From the Ship's Agent: ship husbandry schedule;
From the Operations Manager: vessel schedule

The next activity in the workflow is the every-other day planning meeting with the terminal managers. In this 30-45 minute meeting, each manager[20] presents information they have received in order for the others present to confirm or correct their information. Using this information, the security manager may update his perimeter and personnel security plan.

[18] All personnel wishing to access a marine transportation facility unescorted must possess a Transportation Worker Identification Credential (or TWIC).

[19] The terminal provides an escort to those needing transport between the gate and the vessel.

[20] The terminal has a safety and security manager, operations manager, facilities manager, maintenance and repair manager, and IT manager.

Task: Terminal managers discuss plans
Information Input:
From the Maintenance and Repairs Manager: equipment issues;
From the Operations Manager: unload plan, disposition plan, vessel schedule, labor schedule;
From the Ocean Carrier email: out of gauge cargo;
From the CBP Inspector email: inspection orders, BAPLIE
Information Output:
From the Security Manager: security plan changes

The next trigger is the physical arrival of the vessel. After vessel arrival, the unload plan is carried out. The security plans for manning gates and for escorting personnel are developed to support the unload plan. The unload plan details which containers are to be unloaded and where they are to be placed in the yard. The terminal knows which containers to unload via the COPRAR EDI message[21] and knows where those containers are located onboard the vessel via the BAPLIE EDI message.[22] The terminal uses Navis terminal operating systems Express and SPARCS to control the movement of containers on and between the vessel and terminal yard. As each container is unloaded from the vessel, the container number is entered into Express (a relational database) which syncs with SPARCS (a graphical user interface).

The terminal sends the shipping line either a COARRI EDI[23] or an EDI 322, depending on which standard[24] the company uses, to notify them that the container has been unloaded. The containers with no inspection holds are moved to their place of rest in the terminal yard. Containers that have a CBP hold on them will pass through CBP's vehicle and container inspection system (VACIS) which produces an image of the contents of the container. This container image is compared to the container's cargo manifest, submitted by ocean carrier via EDI 309[25] and accessed by CBP through their ACE (Automated Commercial Environment) system, to determine if further inspection is needed.

[21] The COPRAR is sent from the ocean carrier to the terminal authorizing them to discharge specific containers.

[22] The BAPLIE is prepared by the terminal operators at the vessel's last port of call in coordination with the ocean carrier and the vessel captain. It is passed on to the terminal operators at the next port of call by the ocean carrier.

[23] Acronym comes from its initial use: COntainer ARRIval message.

[24] The COARRI comes from the EDIFACT standard, and the EDI 322 comes from the ANSI standard.

[25] EDI 309 Customs Manifest.

Task: Unload container
Information Input:
From SPARCS: unload plan, COPRAR, container location
Information Output:
From SPARCS: COARRI;
From SPARCS: EDI 322

Task: Scan container
Information Input:
From Express: container ID
Information Output:
To Express: EDI 322;
To SPARCS: EDI 322

Task: CBP drive by scan
Information Input:
From ACE: EDI 309, EDI 350
Information Output:
From VACIS: container image;
To ACE: EDI 350;
To Express: EDI 350

Task: Move container to resting place
Information Input:
From Express: container location
Information Output:
To Express: container location

The next activity is to clear the container for release. The two types of holds considered in this model are CBP and USDA holds. CBP notifies customers, terminals, carriers, and other authorized parties of the hold status via EDI 350.[26] The first task in this activity is to determine where the container needs to be to enable CBP to inspect the container. If the specified location is not the container's current location, then the container will be moved to the appropriate location. The container location is tracked in Express.[27]

CBP will proceed with its secondary inspection which entails an officer scanning the container using sensitive hand-held equipment.[28] The container will either pass inspection, in which case the CBP container hold will be removed, or fail inspection, in which case it will proceed to the CBP devanning inspection,[29] which occurs off-site at a Customs Examination Station (CES). If the container passes the devanning inspection, its CBP hold is removed, otherwise, the terminal workflow is terminated.[30]

[26] The EDI 350 Customs Status Information message is used for all holds and uses a disposition code to denote from which agency the hold originates.

[27] "Navis Express is a comprehensive terminal information management product. . . Express handles a complete range of terminal business transactions such as import and export processing, bookings, gate activity, equipment management, billing, EDI (electronic data interchange), and more." Navis. (2005). Using Navis Express Resource Planning Version 2.8 Document Number 314-0508.

[28] Radiation Isotope Identification Device (RIID)

[29] Devanning refers to the removal of the cargo from the container.

[30] The CBP procedures for failed devanning inspections is outside the scope of the model.

Removal of the USDA hold requires that a CBP officer inspect the container for contaminants. If contaminants are found, the container must be steam cleaned and reinspected; the USDA hold is then removed by CBP. Selected tasks and information flow for this activity are highlighted below.

Task: CBP secondary scan
Information Input:
From ACE: EDI 350, EDI 309;
From hand-held RIID: radiation gauge
Information Output:
To ACE: EDI 350

Task: Certified company steam cleans contaminated container
Information Input:
From Terminal: steam clean order
Information Output:
From Steam Cleaning Company: steam clean receipt

Once all holds are removed, the container is able to exit the terminal via intermodal transport. The intermodal transport activity is triggered by the arrival of a truck at the terminal security gate. The terminal gate guard will check whether the truck driver has a TWIC and confirm he is a driver for an authorized trucking company.[31] The gate guard will conduct passive screening during this process and if anything is suspicious he will proceed to active screening.[32]

Once the driver has passed through the security gate, he will proceed to the main gate. At the main gate, the truck driver interacts with the clerk, who will gather information (*e.g.*, container number, booking number, SCAC[33]) from the driver. The clerk will identify the containers available for pick-up that correspond to the booking number provided by the truck driver.[34] Containers may be unavailable for a number of reasons including unpaid Customs duties and unresolved Customs holds. If a container is available, the trucker will obtain a ticket (a terminal interchange receipt, TIR) with the location in the yard where the container is to be dropped-off and the location of the container to be picked-up.

The truck driver will drop off and/or pick-up a container in the yard, and then drive through the CBP Radiation Portal Monitor (RPM) which passively detects radiation. The truck and equipment are checked for roadability[35] before the transaction is verified by the clerk. The transaction is verified when the truck driver enters his TIR into the ticket kiosk at the out-gate; the information on the TIR is compared in Express to the container in the driver's

[31] Ocean carriers that call at APM Tacoma must supply a list of authorized trucking companies. If a truck driver comes to pick-up a container for an ocean carrier that has not authorized that trucking company, the driver will not be allowed to pick-up the container.

[32] In active screening, the guard may search the vehicle.

[33] Standard Carrier Alpha Code (SCAC) is a unique identifier of motor carriers.

[34] Several containers may be associated with one booking number. The driver will provide the booking number and a container number to the clerk; if that container has already been picked up, the trucker will provide another associated container number until one that is available has been identified.

[35] In 2009, the Federal Motor Carrier Safety Alliance (FMCSA) issued the Requirements for Intermodal Equipment Providers and Motor Carriers and Drivers Operating Intermodal Requirement as mandated by §4118 of the SAFETEA-LU.

possession either via OCR or camera. If the information matches, an equipment interchange receipt (EIR) is printed for the truck driver[36] and the truck then exits the terminal and delivers the container to the prescribed destination. The terminal sends an EDI 322 at this point to notify the ocean carrier and customer that the container has exited the terminal. Selected tasks and information requirements for intermodal transport are shown below.

Task: Conduct main gate procedures
Information Input:
From Truck Driver: container ID, seal number, booking number, tractor and chassis weight, trucking company name, SCAC
Information Output:
From Express: EDI 322;
To Notify Party EDI System: EDI 322

Task: Obtain ticket
Information Output:
From TIR: date, time, container ID, container size, container weight, container location (in yard), trucking company name, booking number, vessel name, port of discharge

Task: Verify Transaction
Information Input:
From Truck Driver: container ID, chassis ID, TIR
Information Output:
From Express: EIR, EDI 322;
To Notify Party EDI System: EDI 322

8.5.3 *Security Information Captured in the Model*

One objective of the model was to discover what security information is used and generated in order for the terminal to complete its cargo operations. Modeling the system with this purpose in mind exposes key security measures in place at the terminal and the information they depend on:

- The ocean carrier must submit the cargo manifest 24 hours before containers are loaded onto the vessel at a foreign port. The information used is the cargo manifest (EDI 309) submitted to ACE.
- CBP must notify the terminal that it intends to perform VACIS exams and itemize which containers to set aside for inspection

[36] The EIR can be used by the truck driver as verification that he delivered/picked-up a container in order to receive wages.

purposes. The information used is the VACIS list which is emailed to the terminal from CBP.

- The terminal can only unload containers that they are authorized to by the ocean carrier. The information used is the COPRAR EDI message visible to the terminal in Express.
- The ocean carrier is notified of any movement of its containers at the terminal. The information used is the EDI 322 sent by the terminal in Express.
- High risk containers are immediately inspected upon unloading at the terminal. The information used is the container image produced by VACIS.
- Sensitive radiation detection equipment and physical inspection are used to identify misdeclared, illegal and/or dangerous cargo. The information used is the radiation measurements and visual inspection results.
- Biological hazards are identified and eliminated before the container may leave the terminal. The information used is the status of USDA hold (EDI 350) visible in Express and ACE.
- Only TWIC holders and authorized truck drivers are allowed to access the terminal to transport containers. The information used is the truck drivers TWIC and the terminal's list of authorized drivers. The TWIC is visually checked by the terminal guard. Authorized trucking companies are established through EDI messages.
- The safety of the truck and equipment is checked before the truck is allowed on public roads. The information used is the roadability check results. The check is carried out by contracted mechanics.
- All containers pass through passive radiation detectors before exiting the terminal. The information used is the alarm, or its absence, from the RPM.
- No container may leave the terminal if there is a CBP hold on it (unless it is being transported by a bonded carrier to an off-site Customs examination station). The information used is the EDI 350 Customs Status message visible in ACE and Express.

A number of conditions determine why information moves through the cargo operations workflow in the way that it does, and these conditions are implicit constraints in our model. For example, regulations, organizational culture and policy, technological constraints, and performers' personal preferences for ways of operating may all impact information flow. Subject matter experts sometimes explain these conditions during interviews with analysts, and we documented such explanations in field notes. However, a thorough understanding of the constraints that shape the business process under study requires additional interviews and background research. Were we using a directed rather than a pure discovery approach to our analysis, a thorough understanding of these conditions would be critical to designing an intervention that explores all possible avenues for process improvement — whether it be a policy, technology, or personnel training. As the purpose of the present model was exploratory, a complete inventory of all of the constraints is outside the scope of this report, however, we have identified a subset of the constraints in the course of our modeling activity:

- The division of responsibilities between the Port and the terminal operator is established in the port governance and financing structure. Many ports act as "landlord", and the terminal operator performs the activities. Some ports, such as the Port of Tacoma, have preferential berths, which can be used by the Port in exchange for favorable tax rates for the terminal.

- Cargo manifests (EDI 309) must be submitted by the ocean carrier 24 hours before a vessel is loaded due to the Trade Act of 2002.

- The requirement that all personnel wishing to access a marine transportation facility unescorted must possess a Transportation Worker Identification Credential (TWIC) is mandated by the Maritime Transportation Security Act of 2002

- The roadability check on all trucks leaving the container terminal is required by the Federal Motor Carrier Safety Alliance (FMCSA) Requirements for Intermodal Equipment Providers and Motor Carriers and Drivers Operating Intermodal Requirement as mandated by §4118 of the SAFETEA-LU (Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users).

- The type of work, hours, wages, etc. of ILWU longshoremen and clerks are fixed in contracts that are negotiated at regular intervals (National Labor Relations Act).

Any proposed intervention would need to perform within these constraints as well as other constraints found in the Phase 1 analysis.

8.6 Discussion

We have presented an exploratory use of the model-based systems engineering approach. Earlier we introduced the idea that our MBSE approach can be used for either exploratory or directed analyses depending on the desired analytical product. We have presented the results of an exploratory analysis and the resulting as-is model of the flow of work and information through the selected use-case. Had we chosen a directed approach and scoped our analysis around a specific problem and intervention, our results would have included a to-be model, meaning a model of how the use-case would change if the intervention were implemented and an analysis of the differences between the as-is and to-be model in terms of resource usage (performer, time, and information). However, as our use-case was selected for discovery and not directed analysis, these additional analytical products are outside the scope of the present work.

From our exploratory analysis we discovered two areas that could be investigated further in future work. Specifically, we will discuss two topics relating to information sharing that were discovered in the model that have connections to current and future federal initiatives. The first topic is that of electronic data interchange (EDI). EDI is pervasive in the trade industry and can inform the current development and industry integration of the National Information Exchange Model (NIEM). The second topic is that of the Automated Commercial Environment (ACE) and the presidential mandate for ACE to serve as a single window between the trade industry and the 48 federal agencies involved in trade.[37] The ACE system was chosen as a discussion point in the year one report because it appears frequently in our model, its use is mandated, and it uses EDI messages. Finally, we will comment on the value of using the model-based systems engineering approach to achieve our objectives.

8.6.1 Electronic Data Interchange

An electronic data interchange (EDI) is the "transmission, in a standard syntax, of unambiguous information of business or strategic significance between computers of independent organizations."[38] EDI software is required to transform information stored on a company's internal systems to EDI standard format. A company can choose to send one or two documents or all of their documents via EDI; similarly they can communicate with some trading partners via EDI and other partners via other methods. The degree to which a

[37] CBP. (2014). ACEopedia. http://www.cbp.gov/sites/default/files/documents/ACEopedia%20August%202014.pdf

[38] Data Interchange Standards Association, INC. (2014). Common Questions about E-Business. http://www.x12.org/x12org/about/faqs.cfm#a1

company uses EDI varies across the maritime industry.

In the model, six EDI messages appear. The first message is the BAPLIE which communicates the position of containers aboard the vessel. The standard definition is

> A message to transmit information about equipment and goods on a means of transport, including their location on the means of transport. The message can be exchanged between (liner's) agents, tonnage centers, stevedores and ships masters/operators.[39]

The BAPLIE is transferred between the ocean carrier, the vessel's captain, and terminal operators at ports at which the vessel intends to call. The BAPLIE contains information about container weight and whether the cargo is hazardous. The position of a container containing hazardous cargo is a safety issue and incorrectly stowed hazardous cargoes[40] have led to maritime casualties.[41]

The second message is the COPRAR which is sent from the ocean carrier to the terminal operator and authorizes the terminal to discharge containers. The formal definition is

> A message to order to the container terminal that the containers specified have to be discharged from a seagoing vessel or have to be loaded into a seagoing vessel. This message is part of a total set of container-related messages. These messages serve to facilitate the intermodal handling of containers by streamlining the information exchange.[42]

The COPRAR is important in security and economic resilience. The COPRAR ensures that the correct cargo is unloaded in the correct place. Containers holding hazardous goods, arms, or ammunition, for example, could cause security issues if they are unloaded at the incorrect port. As for economic resilience, delays in delivering goods to their intended destination will increase costs and could delay the larger supply chain.

The third message is the COARRI message[43] sent from the terminal operator to notify the ocean carrier that the authorized containers have been unloaded. This message allows the ocean carrier to confirm the location of its containers and the shipper to track their shipment.

The fourth message is the EDI 322 which is sent from the terminal operator to the ocean carrier to notify the carrier of container activity, *i.e.*, discharge of the container. The EDI 322

> transaction set can be used to provide all the information necessary for a terminal operation, port authority or intermodal ramp to communicate terminal and intermodal ramp activities (*e.g.* , in-gates and out-gates) to authorized parties to a shipment.[44]

This message keeps the ocean carrier aware of what is happening to their container and increases transparency of container activity.

[39] United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT). (2000) BAPLIE. http://www.unece.org/trade/untdid/d01a/trmd/baplie_c.htm

[40] Due to misdeclaration of cargo.

[41] Foster, C. (2007). Misdeclared or Undeclared Dangerous Goods Cargoes. Swedish Club Letter.

[42] United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT). (2000) COPRAR. http://www.unece.org/trade/untdid/d01a/trmd/coprar_c.htm

[43] United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT). (2000) COARRI. http://www.unece.org/trade/untdid/d00a/trmd/coarri_c.htm

[44] The Accredited Standards Committee (ASCX12). (2002). X12I Version 5 Transaction Set Tables: 322 Terminal Operations and Intermodal Ramp Activity. Pg. 71. http://www.x12.org/x12org/subcommittees/X12i/I0000_ANSV5_Trans_sets_A.pdf

The fifth message is EDI 309 Customs Manifest. This EDI is sent from the ocean carrier to CBP to satisfy the 24-hour advance vessel manifest rule. The EDI 309

> transaction set can be used by carriers, terminal operators, port authorities, or service centers to provide Customs with manifest data on cargo arriving in or departing from oceangoing vessels, railroad trains, or other types of conveyances. The transaction set can also be used by carriers to provide terminal operators, port authorities, or service centers with manifest data on cargo arriving at their facilities via the conveyances mentioned above.[45]

The ocean carrier submits one EDI 309, which contains individual bills of lading from separate shippers, before the vessel leaves the first foreign port at which it loads cargo, *i.e.*, the first export port. As the vessel loads additional cargo at following port calls, additional EDI 309s are sent for each cargoes' bill of lading.

The sixth message is an EDI 350 sent from CBP to other interested parties to notify them of various CBP actions, *e.g.*, hold placed on container, hold removed from container. The EDI 350

> transaction set can be used by the Customs Service (CS) to supply carriers, terminal operators, port authorities, and service providers with cargo release and cargo hold information for import shipments. It can also be used by the CS to provide exporters or their agents, carriers, and service providers with information pertaining to export shipments.[46]

Prior to receiving this EDI, the container may not leave the terminal facility unless it is going to an external examination station. The hold status is visible on the terminal's website for external parties to periodically check. This EDI has economic implications; if a truck driver arrives at the terminal to pick-up a container that has not been cleared, the customer/freight forwarded will need to pay for two trips to the terminal.

Other EDI messages are used by the ocean carrier, terminal operator, motor carrier, and customers but fall outside of the scope of the model. One example of an out-of-scope EDI is the EDI 300 Booking Request which is sent from a shipper to the ocean carrier requesting a booking.[47] Another example is the EDI 204 Motor Carrier Load Tender which is sent from a shipper to the motor carrier requesting their service to move a container.

Not all companies choose to use EDI, due to its significant cost, so alternate methods of computer-to-computer data transmission[48] must be supported. The current version of CBP's Automated Commercial Environment (ACE) system accommodates companies that do not wish to use EDI. The system allows users to interact with it through either EDI or the ACE Portal. The ACE Portal requires the user to

[45] The Accredited Standards Committee (ASCX12). (2002). Transaction Set Tables: 350 Customs Status Information. Pg. 61. http://www.x12.org/x12org/subcommittees/X12i/I0000_ANSV5_Trans_sets_A.pdf

[46] The Accredited Standards Committee (ASCX12). (2002). Transaction Set Tables: 350 Customs Status Information. Pg. 78. http://www.x12.org/x12org/subcommittees/X12i/I0000_ANSV5_Trans_sets_A.pdf

[47] A booking is a reservation of space, containers, and equipment needed to transport goods via vessel. The Accredited Standards Committee (ASCX12). (2002). Transaction Set Tables: 300 Reservation (Booking Request) (Ocean). Pg. 52. http://www.x12.org/x12org/subcommittees/X12i/I0000_ANSV5_Trans_sets_A.pdf

[48] fax, email, and web interfaces

manually input data. One trucking company interviewed uses EDI to communicate between the main office and the on-board truck computers, but their EDI software is incapable of communicating with ACE, so they use the ACE Portal to communicate with CBP.

The cargo operations model exposes the varying use of EDI and reinforces the need for federal systems to support non-EDI methods of information sharing. Entities that do not use EDI messages are still influenced, however, by the standards when sharing information. The EDI standards define common data elements and ensure the community has a common vocabulary.

A current federal initiative to standardize the format of information exchange is the development of the National Information Exchange Model (NIEM) which serves as a data model and reference vocabulary.[49] Data models describe the data needed and created by business processes.[50] Our cargo operations model can be viewed as a conceptual data model that captures the information flow needed to successfully complete the business process of facilitating trade.

The National Maritime Domain Awareness (MDA) Architecture Plan is the federal plan for information sharing and safeguarding.[51] The plan aims to define what information will be shared, with whom, and by what methods in order to support policy. It consists of a common language, common security, and common environment. The common language is the National Information Exchange Model (NIEM) which is "a standard way of defining the contents of messages being exchanged."[52] The common environment is the Maritime Information Sharing Environment (MISE). MISE encourages understanding before building:

> Successful information sharing activities are the result of operational, information and technological understanding achieved through a well-defined and routinely implemented process[53].

The MISE method of achieving this understanding starts with (1) describing an operational use-case and (2) identifying the essential data elements supporting the use-case. The cargo operations model satisfies these two MISE needs for the particular use-case. The information dictionary produced from our model consists of the essential data elements and the work to which they are critical. The model built in Phase 3 aligns well with the National MDA Architecture Plan's prescribed method of achieving data compatibility.

8.6.2 *International Trade Data System and ACE*

An example of current federal initiatives that impact our Phase 3 use-case is the International Trade Data System (ITDS). We encountered

[49] Bureau of Justice Assistance (BJA) and the NIEM Project Management Office (PMO). (2007). National Information Exchange Model (NIEM) User Guide Volume 1.

[50] West, M. (Ed., Fowler, J). (2003). Developing High Quality Data Models, Prepared for European Process Industries STEP Technical Liaison Executive (EPISTLE).

[51] National Maritime Domain Awareness Architecture Plan. (2013). Version 2.0, Release 3.

[52] Frank, S. and Radlinski, T. National MDA Architecture Plan Brief

[53] Frank, S. and Radlinksi, T. Maritime Information Sharing Environment: An Information Exchange. Brief to Mr. DeVries, Office of the DOD CIO. August 13, 2013.

the ACE component of ITDS throughout our model and briefly discuss it here. A deeper, focused analysis would need to be conducted to determine ITDS's future impact on the trade community.

Mandated by the SAFE Port Act of 2006, the International Trade Data System is an information system built as part of CBP's Automated Commercial Environment (ACE) trade processing project. The purpose of ITDS is to streamline data processing and information exchange among commercial entities and participating government agencies (PGA) around imports and exports. ACE aims to provide a "single window" through which all information can be exchanged electronically and is intended to leverage several data exchange standards including the Electronic Data Interchange (EDI) and the National Information Exchange Model (NIEM). Implementing ITDS includes the following mandatory milestones to be completed within the three years following this report:

- May 1, 2015: Mandated use of Manifest - All electronic export and import manifest data must be transmitted via ACE.
- November 1, 2015: Mandated use of Cargo Release - All data associated with the release of cargo, including PGA interactions, must be transmitted via ACE.
- October 1, 2016: Mandated use of ACE[54].

The success of ITDS through the use of ACE depends on participation of traders and PGAs. The information environment in which international trade operates is heterogeneous. In our investigation, we discovered very limited use of ACE and variable use of EDIs. We did not encounter any mention of the NIEM standard in use. Currently, ACE is an "opt in" system requiring a paid subscription, and it is not widely utilized. The 2013 ITDS Report to Congress points to technical reasons for this, specifically that software for retrieving data has not been perfected and has capacity limitations. However, the reasons that technology adoption fails are often cultural and social-rarely are they purely technical. One non-technical reason pointed out in the report is that "... the Portal (ACE) does not supply data of interest to some agencies."[55]

Although ACE has developed system-to-system interoperability (interoperable web-services) for commercial partners, this will not help companies that do not currently submit their documentation electronically. Many of the processes that ACE is designed to streamline have "historically been done entirely manually and [are] paper-based" (*e.g.*, cargo release, the submission of export manifests). The difficulty of transitioning from paper to electronic documents is well documented in other health and safety critical

[54] CBP. (2014). ACEopedia.

[55] Report to Congress on the International Trade Data System. (2013).

domains (*e.g.*, healthcare and aviation), and workflow modeling, such as the approach we present, has proven a useful strategy for minimizing the disruption caused by such transitions.[56] In our modeling investigation, we discovered that there is wide variability in the technological capabilities of trucking companies, and while some have adopted electronic information exchange models (EDI), many others continue to transmit their information via mail, phone, or fax. By pinpointing precisely when and where information flow relies on non-electronic documentation, we can begin to understand and plan for how the transition to electronic documentation will impact the work.

Unlike many commercial entities, most PGAs currently transmit information electronically. For PGAs in this category, including the U.S. Coast Guard, the roll-out of ACE will not mean using the IWS to translate information, but rather the adoption of the ACE system and interface and the workflow it imposes. These PGAs may not need to manage a change from manual, paper to electronic processes, but they may need to plan for the transition from their own organization's process to the process imposed by the new ACE system.

One branch of the U.S. Coast Guard that will likely be affected by the roll-out of ACE is Inspection, particularly personnel who inspect international vessels. We are well poised to expand our current model in this direction, and we have conducted preliminary interviews with USCG vessel inspectors toward this aim. In these interviews, we learned that the U.S. Coast Guard inspectors' current processes for reviewing importers' and exporters' documentation, and for conducting and documenting inspections currently requires an intricate dance across paper and electronic documents. So even though the intention behind ITDS' mandate that all information be exchanged electronically is to make the process more efficient, the elimination of paper will have a significant, yet unknown impact on U.S. Coast Guard inspectors' workflow.

Expanding the model to include an analysis of U.S. Coast Guard inspectors work including facility as well as vessel inspections could also shed light on a known problem in the flow of security information at the U.S. Coast Guard, specifically, the documentation of port facility inspections. In 2008, the Government Accountability Office (GAO) found a discrepancy in the number of inspections that were required to be conducted and the number that were actually documented.[57] In 2011, the GAO recommended that the U.S. Coast Guard develop "policies and procedures to ensure that annual security inspections are conducted and information entered into databases is more useful for management."[58] The U.S. Coast

[56] Leviss, J. (2009). H.I.T. or Miss: Lessons Learned from Health Information Technology Implementations. *AHIMA*.

[57] Government Accountability Office. (2008). Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data. (GOA Publication No. GAO-08-12). Washington D.C.: Government Printing Office.

[58] Government Accountability Office. (2014). Maritime Security: Progress and Challenges with Selected Port Security Programs. (GOA Publication No. GAO-14-636T). Washington D.C.: Government Printing Office.

Guard concurred with this recommendation and told GAO that they have plans to improve their inspection database by March, 2015. Such improvements pose yet another potential disruption to the information environment that our model has positioned us to investigate.

8.6.3 *Methodology Discussion*

The main methodological conclusion from Phase 3 is that the model-based systems engineering approach acheived our goal of community-driven understanding of the use-case. In the cargo operations use-case this manifested in the discovery and documentation of the usage of security information in container terminal cargo operations. Our methodology adds value in several distinct ways:

Discovery: Workflow modeling increases accuracy to identify the information that is actually used in mission accomplishment. It adds important context that aids recollection of information use, as compared to conventional methods, such as focus groups. Also, by treating information as a resource, instead of a task, workflow models are more tractable in size and complexity.

Workflow modeling also reveals inconsistencies or gaps in our understanding, which can be addressed in follow-up interviews or observations. Our methodical technique of stepping through the workflow to identify needed information provides a technique to cross-check for greater thoroughness of both tasks and information needs. This iterative part of our method increases its focus for cost-effectiveness. These features of systems modeling provide an important complement to the methods used in Phase 1.

Automation: Automated generation of an information dictionary is another cost-effective feature of our modeling tool. The dictionary indexes information attributes to each of the tasks where they are used, giving some indication of the value of that specific information. It also indexes the information to the immediate information resource, which reflects the value of the resource. Redundant information resources often add overhead cost to manage and keep them synchronized.

The information dictionary has important implications for standardizing information types/usage, *e.g.*, NIEM and EDI. Our Phase 1 findings show uneven and limited adoption of relevant information standards. Analyzing new information standards in the context of the operations they must support should give more accurate and economical direction to focus effort.

Generality: Generality is an important dimension to evaluate modeling methods. The generality of the results and the generality of the method are both important here. As with any new method, replication will be needed over a wider variety of use-cases to understand how general the method is in terms of the situations where it should be applied. The modeling tool, itself, was designed to permit re-use of models, so each subsequent project can increase the cost-efficiency of the method. For example, the generality of the specific APM model depends on how representative APM is of container cargo terminals. Since APM does not have pipeline nor on-dock rail, any conclusions should be limited to container operations. The flexibility to model the role organizations play as information resources is an important advantage that allows us to proceed incrementally when we do not yet know enough about their internal processes.

Cost-Effectiveness: Our method for model-based systems engineering requires moderately high levels of skill in several areas: planning and carrying out semi-structured interviews, analyzing existing information resources and standards, and systems modeling in a diagramming language based on the BPMN standard. This combination of high skills pays off by needing less time from the personnel who work in/around cargo operations. This is an important practical factor since voluntary cooperation of businesses and agencies is essential to the success of any modeling project and their time is scarce.

Terminal operations were the selected focus of Phase 3. The model included participation of trucking companies on-site to deliver and remove containers, but none of their internal processes. The ocean carriers were represented as information resources, as were state/federal regulatory agencies. Year 2 MOISA provides an opportunity to expand the model with the workflows that account for how the information is generated within these organizations. This technique gives our method excellent, incremental scalability.

Scalability: Scalability, however, is traded-off against scope and the level of granularity needed to document security information usage. The APM model captures only enough scope and detail of cargo operations needed to reveal the usage of security information and how that constrains operations. Other potentially interesting aspects of operations were deliberately avoided in order to satisfy that objective. Information usage reflects policy for access to information resources, as well as the contents and usability of the resources, themselves. This trade-off makes the scalability practical, but sacrifices detail about tasks that do not use or change security information.

Information resources, like other types of resource, constrain the way people can use them to do their work. A workflow reflects many other factors as well, but our method shows how, given those conditions, a given set information resources impact a work system. We have identified three possible strategic options to take advantage of this principle in year two:

1. Understanding and problem discovery: understanding what information is actually used, where it is used in operations workflows, and how the resources that provide it constrain operations (as demonstrated by the results of our current Phase 3).
2. Problem investigation: A given problem area in operations could be specified, and our method could be applied as a cost-effective way to diagnose the role of current information resources and analyze options to mitigate or eliminate the problem, *e.g.*, ongoing information sharing issues between USCG search and rescue and 9-1-1 centers.
3. Evaluating the impact of new information resource: A model of current operations could be analyzed for the impact of a new information resource during its design stage. This formative evaluation would guide design decision making to prioritize functionality by positive impact and identify negative impacts and assist to design ways to avoid or mitigate them, *e.g.*, the impact of an MCOP roll-out or CSSE.

8.6.4 Business Process Modeling Toolkit

The Business Process Modeling Toolkit (BPMT) is a new web-based application under development that will allow operations/business leaders to create visual models of workflows using standardized graphical elements based on the Business Process and Model Notation (BPMN). BPMT will save the elements of the model to a central database and recall them for subsequent simulation and analysis. The goal of BPMT is to better reveal to stakeholders how IT should be applied, not only to make the flow of information more synergistic with maritime operations that use it, but also in terms of service outcomes and client satisfaction.

The experience of applying MATH in Phase 3 fed into the requirements development for BPMT to replace the MATH suite of applications (MATHFlow, MATHSim, and MATHView) originally developed ten years ago for the healthcare industry. MATHFlow currently interacts with Microsoft Visio to allow the user to build a BPM while simultaneously recording a schematic model in a Microsoft ACCESS database that can be read by MATHSim and MATHView. MATHSim performs Monte Carlo simulations to measure the performance of the workflows, allowing several models to be compared against one another. MATHView provides automatic clustering methods that allow UML data structures representing information architectures to be derived for use in software design/development.

During MOISA Phase 3 we began analysis and design of BPMT for all the functionality of the above trio of tools, redesigned as a web-based application that no longer relies on Microsoft Visio or ACCESS. This will enable a far more efficient, friendly, and useful delivery of future models to stakeholders. We developed a System Requirements Specification (SRS) document that describes in detail the overall functions of BPMT, the potential users, their roles and tasks, and the software requirements and capabilities.

9 Discussion, Conclusions, and the Way Forward

9.1 *Discussion*

Year one of MOISA was a collaborative effort with the Puget Sound maritime safety and security community to answer the question: What is the nature of the community's day-to-day operational information sharing environment (ISE) and what is the role of that ISE in achieving their collective missions? In a broad, general sense, the community's answer was simple and nearly unanimous: "When it comes down to it, it is all about relationships." This answer, repeated so many times in so many ways, may sound simplistic and unrelated to the predominately data-focused, technology-based approaches to enhancing the ISE, yet it and associated answers about the nuanced, dynamic, self-organized, highly informal, trust-based nature of the community's operational ISE have profound implications for the safety and security of our nation.

While the maritime community's focus on human relationships, and the ability of these relationships to support highly nuanced information sharing, may sound unrelated to high tech security systems based on sensors, communications technology, data integration, interoperability, detection algorithms and visual analytics, these state-of-the-art technology-based initiatives wrestle with the same issues of trust and information access (*e.g.*, identity and entitlement management). Furthermore, these technology "solutions" are dependent upon acceptance and use within the community's operational ISE for sustained existence and meaningful impact.

The community told us how hard it works on a day-to-day operational basis to align their ISE with the work being done in support of their missions. They also told us of the many ways in which technology-based initiatives have not been aligned with that work; how important information will not be shared if it cannot be qualified or non-attributable in ways not supported by formal systems; how in some cases, critical information could only be shared by going around those systems, not through them. Technology interventions that are not aligned with the community's day-to-day operational work cannot survive.

This does not mean that systems based on information and communication technology cannot enhance Federal efforts to achieve "national security through responsible information sharing"[1] or to "advance maritime intelligence integration, information sharing, and domain awareness to foster unity of effort for decision advantage. . . "[2] or to "improve multi-agency maritime security operations and enhance cooperation among partner agencies"[3]. It does mean that to get a return in regional safety and security from investments in these systems, they must be appropriately designed and implemented through methods that center on humans, community, and work. Over the past year, the community has told us that past initiatives in a series of technology-based solutions have had little sustained impact on their ISE and its ability to support enhanced safety and security. It is clear that throughout the life-cycle of technology intended to enhance the regional ISE, designers, developers and sponsors need to address the informal as well as the formal, the diverse day-to-day operational environment as well as the centrally structured NIMS environment, the human as well as the technological.

The Puget Sound community's ISE during day-to-day operations is like a fabric, woven through past shared experiences and continually being strengthened through collaborative work (much of which is economic rather than security driven), regional planning, exercises, meetings, social gatherings and conversations over coffee. The community views the quality of this largely self-organized fabric as a key element of regional resilience in the face of threats to safety and security. They work hard to maintain and improve this fabric, increasing their self-knowledge of the community because this self-knowledge is central to their readiness to work quickly and effectively as a team, whenever the need arises and whatever the situation being encountered.

Of course the ISE of day-to-day operations is not the same as the ISE of incident response. We found that most members of the community do not on a day-to-day basis see security as their job one. Even a police interviewee identified his primary job as community relations. day-to-day operations occur at a different pace and focus than the intensity and time pressure of life-saving incident response. day-to-day operations are highly motivated by economics, including barriers to information sharing due to competition that are set aside during incident response. Yet despite these and other differences, the ISE of day-to-day operations and the ISE of incident response are

[1] PM-ISE Vision

[2] NMIO Mission

[3] IOC Description

intimately intertwined.

The NIMS relationship framework, even during incident response, does not replace the importance of the self-organized, extremely rich and nuanced, informal community fabric of identity and trust. As the previous Captain of the Port put it, holding up his NIMS manual and introducing an earthquake exercise, "This is our going in position." Once an incident occurs, the community still relies on its fabric of trust to coordinate and innovate, perhaps even more so. The community views this ability to coordinate and innovate, based on the ISE that they have exercised and worked to improve on a day-to-day basis, as their greatest asset.

Despite the community's focus on its relationship-based operational ISE, there are still critical gaps in this fabric. There are gaps from personnel turnover and retirement, from stove-piped thinking and investment, from conflicting priorities and missions and cultures. Where gaps exist, regional resilience is decreased. This is because gaps in the community fabric of trust and self-knowledge; gaps in the framework for information sharing; gaps in the understanding of who needs what, when, how and whether or not they should receive it; translate into less effective and responsive action by the community. For this reason, the most significant part of day-to-day operations in terms of the impact on safety and security is the community's ongoing work to establish trusted relationships and self-knowledge.

There are numerous formal systems in the Puget Sound region intended to receive, store, and deliver incident-focused information. The parts of those systems that come closest to addressing the day-to-day operational work of the community are identity and entitlement management — who are you, can I trust you, what can I appropriately share with you? In terms of systems design, development and use, this is a major focus of national initiatives to improve the ISE, but it appears to be far less of a focus of the diverse regional community. The community shows little interest in or awareness of data standards or meta-tagging or national exchange models. Perhaps this is because they are working on a day-to-day basis to develop a nuanced and non-technology based system of identify and entitlement management, or because we found many examples where they needed to work around existing formal frameworks to get their day-to-day operational job done.

Initiatives to improve the regional ISE for safety and security need to understand the existing informal ISE of day-to-day operations. Federal-centric formal systems, delivered as a series of technology-based solutions, have not supported the day-to-day work and mission of the community, nor have they supported the strengthening of community fabric and self-knowledge. In the past, these systems have been brought in piecemeal with few plans for sustainability. They have added new work; made current work harder, not easier. They have not been owned by the community as a whole, not designed based on a thorough knowledge of how the regional community works, how they share information, and how they self-organize. They have introduced constraints and had unintended consequences, addressed one problem of a complex, highly interdependent system (usually a problem of the Federal component) at the expense of introducing new issues elsewhere in the system (usually at the local level).

But they could. Despite years of attempting to accommodate a series of federal solutions, despite continually following directives that require the locals to put information into formal systems, with little or no reciprocal return of information of use to regional efforts, despite a Federal funding strategy that leads to fragmented and duplicative efforts with no long-term strategy, the regional community still looks to the Federal component for support and guidance. The regional community still pleads for rational policy and true partnership. Who else is in the position to provide it?

There are critical questions to be answered. What will it take to align federal investment in safety and security with regional work and practices to better achieve that safety and security for its citizens, institutions, and infrastructure? What will it take to achieve community acceptance and ownership of future solutions and strategies? How can these solutions and strategies be sustained, improving over time and use rather than degrading as they currently do?

In Phase 3, MOISA demonstrated a methodology for achieving a more holistic, human-centered approach to enhancing security systems. This demonstration was based on process modeling of a container terminal's cargo operations, centered on humans, their work, and their use of information to accomplish that work. While not the only approach, Phase 3 gives insight into the need to base future security system enhancements on a deeper understanding of the complex system by which that security is currently being delivered, as well as on a deep involvement of the community currently delivering that service.

Perhaps the long-term answer to the above questions lies in an integration of the perceived dualities of formal and informal work, of online technical activity and offline human activity, of day-to-day operations and emergency response, of central and local, and addressing these challenges more holistically, recognizing their existence within an interdependent and dynamic socio-technical system. This is not easy, but there are emerging fields of human centered design and engineering dedicated to achieving this goal. These fields are given impetus by the growing realization, in the context of failures like Microsoft VISTA and the troubled healthcare system roll-out, that if you cannot afford the time and resources to do it right the first time, you certainly don't have the time and resources to do it over again. . . and again.

Hopefully MOISA is an important step towards long-term, sustainable enhancement of our nation's safety and security systems, based on a mutual understanding of the rich partnerships and information sharing in operation every day across the diverse community charged with this precious task.

9.2 Conclusions

The following are specific conclusions that emerged from the MOISA analysis of the Puget Sound maritime safety and security community's information sharing environment. Conclusions are presented under nine overlapping categories: (A) features of day-to-day operations, (B) focus on security, (C) nature of collaborative relationships, (D) nature of information, (E) structures for information sharing, (F) technology, (G) concern for economic impact, (H) alignment with national-level initiatives, and (I) funding.

A. Features of day-to-day Operations

- Safety and security are generally part-time activities.
- Safety and security issues are 24/7.
- Information sharing is generally informal.
- Information sharing is generally self-organized.
- Information sharing is generally based on relationships built during non-emergency work.
- The information sharing environment (ISE) built during day-to-day operations is a critical component of emergency response and management.
- The work of aligning the resources and building the capability to respond to incidents occurs outside the context of an incident.
- Successful information sharing requires expertise in the community itself.

- Long-standing community members, many of whom have held multiple positions in multiple organizations, have tacit knowledge and expertise about the community itself that makes them critical nodes in the ISE.

- There is considerable diversity in modes of communication that complicate the day-to-day ISE.

- Day-to-day operations are generally decentralized. Individuals and organizations carry out multiple tasks in service of multiple, sometimes misaligned, objectives.

- Authority is bestowed upon information leaders — individuals who have expertise in the community and knowledge of the work at hand.

B. Focus on Security

- For most community members, security is not the primary focus of their day-to-day work.

- Community members, particularly those in the private sector, are often unaware of how their day-to-day operations relate to security.

- Day-to-day activities related to safety and security are driven by an awareness of risk, *i.e.*, they are driven by the need to prepare for possible incidents.

C. Nature of Information Sharing

- The quality of the community ISE is woven together in a fabric of relationships, individually recognized expertise, and shared experiences.

- The community is self-organized in that community members themselves identify, establish, and maintain relationships with their preferred collaborators.

- Knowledge of the community and its work is a prerequisite for identifying and understanding what relationships are important and how to establish and maintain them.

- Trusted relationships take time (often years) to establish. These relationships change over time, and thus, so do the information sharing practices that support these relationships.

- Trust among community members is the foundation of effective information sharing.

- The ISE fabric is not generally achieved through formal definitions and agreements embedded in policy and IT systems. If fact, liability and policy issues can hinder information sharing.
- Face-to-face communication, which includes meetings, conferences, and joint exercises and drills, is highly valued by the community.
- Identity and entitlement management are primarily community properties.
- Community members are hesitant to enter into formal information sharing agreements where no previous relationship existed.
- Agencies select MOU/MOA partners based on individual relationships across organizations.
- There are some qualities of information sharing partnerships that are specific to different sectors. For example:
  - Industry and commercial agencies feel left out of information exchange.
  - Information sharing relationships can be difficult to establish between tribal and non-tribal entities.
  - There is a cultural gap between land and maritime entities that impacts information sharing.
  - Communication between the Federal Government and non-federal entities is viewed as one-way-information is shared with federal agencies, but the federal agencies do not share back.

D. Nature of Information

- Information critical to day-to-day operations comprises both quantitative and qualitative data.
- Structured data and the formal systems that hold it, are viewed as lacking flexibility.
- Security clearances create difficulties in information sharing.
- Many elements of information that are critical to safety and security at the regional level are dynamic, diverse, nuanced, informal, and trust-based. These elements cannot be captured in current structured data formats at the enterprise level.
- Too much information is often viewed as more of a problem than a lack of information.
- Information ownership affects access.

E. Structures for Information Sharing

- Informal leadership structures are an essential component of the fabric of the community and critical to the success of day-to-day as well as incident-focused operations.
- Supporting the core security work of the community during non-crisis times is critical to reducing risk during a crisis.
- Subject matter experts (“information leaders”) despite rank or title are key decision makers and key information sources.
- Informal leadership structures operate 24/7 and neither these structures nor the role of information leaders disappear when an incident occurs.
- During an incident, as soon as working under formal structures appears to slow or impede operations, people often default to working with information leaders and the informal leadership structures that support them outside of incidents.
- Changes in leadership and high turnover rates disrupt the personal relationships that the maritime community so heavily relies upon.
- From the perspective of the community, the national security system and its extensions into law enforcement information is not the keystone of identity and entitlement management.
- Home Rule status is viewed by many members of the community as supporting the tendency for day-to-day operations to be less formal and more fragmented.

F. Technology

- Technology is viewed as a secondary strategy in overcoming challenges to the community information sharing.
- Past IT solutions are not generally perceived as having solved information gaps.
- Technology is often perceived as an asset, but not a complete solution.
- The IT component of the ISE is small and is as likely to impede safety and security operations as it is to help, particularly when new “solutions” are introduced.
- Technology is often not adopted because it introduces considerable overhead tasks.
- Technology is often perceived as a headache and dismissed without a full understanding of its potential.

- Most agencies do not have in-house IT personnel.
- Funding and efforts to develop regional SA-COP technology have not successfully been aligned with the gathering and analysis of information to achieve situational awareness that community members engage in day-to-day.
- Community members do not generally rely on SA-COP technology to achieve situational awareness but more typically use basic information and communication technology including phones, email, and radio, as well as relying on their personal, trusted relationships.
- Systems being built using port security grant funds are not required to use common data standards.
- The community believes there are too many systems intended to achieve similar purposes.
- The large number of systems requires multiple passwords, which causes frustration, is inefficient, and may result in security vulnerability.
- New technology is not always reliable and the field can feel like it is being used as a test bed rather than having their work facilitated.

G. Concern for Economic Impact

- In day-to-day operations, ownership, competition, economic impact, and the sustainability of operations effect information sharing.
- In the commercial sector, there is friction between industry sensitive information and the need/desire to share this information.
- Companies that are in competition with one another don’t want to share information that would give a competitor an edge.
- Even state, local, and Federal Government entities sometimes feel that they are in competition for resources and may be hesitant to share information about the resources that they do have or information that might impact the credit they receive for their activities.

H. Alignment with National-level Initiatives

- Information that is critical at the local level often is not captured in common data architectures handed down from national stakeholders.

- Federal policy and regulatory changes are often not well communicated or understood by agencies.
- The community sometimes perceives national-level initiatives as not sensitive to local needs.

I. Funding

- Funding to facilitate information sharing has largely been tied to incidents and is not seen as available to support day-to-day activities.
- Incident-driven activities do not always support day-to-day activities.
- Systems that are not in use day-to-day will not suddenly be adopted in the event of an incident, and solutions designed only to support incident action are not adopted in day-to-day activities.
- The community expressed a need for funding to support day-to-day activities such as training, system maintenance, and support for personnel.
- The community perceives that it is harder to get funding to support day-to-day activities than it is for incident-response.
- The short-term nature and un-reliability of grant funding makes it difficult to use in support of activities that aim to build long-term collaborative relationships.

9.3 The Way Forward

The way forward will require refining aspects of the current relationship between the federal and regional components of the FSLTIPP. To achieve this new relationship and new ways of enhancing the regional ISE, we recommend that appropriate elements of the Federal Government:

- Provide resources not only for initiatives that support incident response and management, but also support the continuum of daily operations that are critical to enhancing the ISE. These activities should be understood as a single operational environment, not competing activities.
- Leverage the current ways that the ISE is successfully established and maintained, *e.g.*, IT systems that support community trust building and self-knowledge.

- Employ project methods that address community identified opportunities for ISE enhancements and produce evidence-based, predictable improvements in security and safety mission performance.
- Base any ISE enhancement on a clear understanding of the work and information sharing environments within which the enhancements must live and evolve.
- Invest in regional community participation and leadership in the design of ISE solutions that will cultivate community ownership of these solutions.

These approaches will empower the regional security and safety community to play a strategic role in the design of their future ISE.

Potential MOISA-specific projects that could move this agenda forward include:

1. **Expand MOISA:** Conduct MOISA in other maritime regions; examine cross-regional best practices and the valuable similarities and differences among them.
2. **Expand Engagement with the Puget Sound Maritime Community:** Based on our year one results, expand the analysis of the current ISE, including expanding the interviewee pool and revisiting some entities.
3. **Develop and Employ New Capabilities for Coordinated Regional Assessment and Deployment of Potential ISE Enhancements:** Develop a regional test bed that demonstrates new methods for collaboratively improving the regional ISE.
4. **Apply Model-Based Design to Community-Identified Information Sharing Challenges:** For example, address an identified information gap between 9-1-1 and USCG SAR by working closely with practitioners to model the as-is work and information flow and produce an evidence-based improved to-be model representing a cost-effective solution.
5. **Explore Sustainability Issues:** Develop design strategies that enable the community to continue to adapt solutions after they are fielded.
6. **Region-Specific ISE Needs:** Explorecommunity-identified information gaps in the context of daily operational needs. For example:
   (a) *Radio interoperability* - analyze reported communication failures and support the community in identifying mechanisms for expanding regional radio interoperability that supports day-to-day mission accomplishment.

(b) *Sensors and sensor data* - Support the community in developing an inventory of available regional sensor data and a plan for using that data in support of day-to-day operations.

(c) *Situational awareness and common operational picture* - Support community assessment of the various SA/COP regional initiatives with an eye towards determining the desirability and feasibility of a single regional system for SA/COP that supports day-to-day operations and is used on a day-to-day basis.

(d) *Essential Elements of Information (EEI)*- Support King-county led initiative to define regional technology-agnostic EEIs.

7. **Funding Alignment:** Examine federal funding practices and policies, with emphasis on understanding how community-based processes are valued. Explore with the community a collaborative mechanism for achieving alignment of federal, state and local investments.

8. **Explore Applications of MOISA to Federal Coordination Initiatives such as NIEMS:** Explore how modeling the regional community's work and information flow can generate NIEMS terms.

9.4 The Takeaway

WHILE the Maritime Operations Information Sharing Analysis project (MOISA) was motivated in part by the desire to explore "information gaps and resource inefficiencies limiting the day-to-day operational effectiveness of major ports," [MOISA Statement of Work] the focus of year one was a descriptive, almost anthropological, effort to understand the complex day-to-day operational information sharing environment (ISE) of the Puget Sound safety and security community. During MOISA Year One (MOISA1) we made no assumptions of problems or inefficiencies; rather we facilitated the community's articulation of how, on a day-to-day basis, it works to make the region more secure and resilient and how it shares information in support of that mission.

Yet despite this descriptive focus (or more likely because of it), MOISA1 produced fundamental information with immense actionable implications for the safety and security of our country. We achieved a deep understanding of how a major region shares information to deliver and maintain day-to-day safety and security for its economic and societal well-being. This understanding reveals a critical need to rethink how we launch, conduct, deliver, and maintain initiatives designed to enhance regional safety and security in the context of an ever-changing security environment. The results of MOISA1 indicate how we can vastly increase the value of these initiatives, particularly when they revolve around information and communication technologies. At the most general level, MOISA1 points towards a desirable redefinition of the partnerships among the diverse federal, state, local, tribal, international, private, and public (FSLTIPP) entities responsible for day-to-day operations that maintain the safety and security of a region.

On a day-to-day operational basis, the current ISE of the people and organizations charged with Puget Sound safety and security is highly informal, based largely on communities of trust that continually evolve through ongoing relationships and shared experiences. It was not long into our exploration of the regional ISE before it became apparent that past investments in security IT systems have not improved the ISE in any way proportional to the size of those investments. This is not to say that IT cannot accomplish the job. MOISA tells us that it is the way we are going about it that is holding us back, not the effort to do so.

The takeaway of MOISA1 is neither that the regional safety and security community does not rely heavily on IT for its ISE (they don't) nor that federal IT initiatives do not sufficiently consider their impact on the work and information flow of the field (they don't), but that these observations are pieces of a larger story of why, after decades of federal investment, IT-based security initiatives have not achieved their intended impact.[4] The point of MOISA is that it could, and our results point out the critical role of the regional community in the way this can be achieved.

Before immersing into the regional community's ISE, we tended to think of misaligned investments across funded regional initiatives, that is, a particular investment does not leverage a previous investment to accomplish the same or similar objective. This type of misalignment does occur (*e.g.*, the multiple Port Security Grant Program funded common operating pictures in the region that do not share data) and is definitely impactful. However, MOISA ended up pointing to another, even more critical, investment misalignment — the misalignment between, on the one hand, the funding, design, development, implementation, and maintenance strategies of federally-funded IT security initiatives, and, on the other hand, the work, information sharing environments, and mission accomplishment of the people and organizations charged with the day-to-day safety and security of their region. The mismatch between the strategies of IT initiatives and the ISE of the operational community doom these initiative to limited, if any, long-term value.

[4] Similarly, investment in health IT has not produced the predicted cost and outcome benefits.

MOISA1 is not telling us that information and communication technology cannot make us more secure, safer, and resilient. Rather, MOISA1 tells us that IT is not now significantly doing so at the regional operational level. Even more importantly, MOISA1 provides knowledge that points towards approaches and methodologies that can align future federal safety and security IT investments with the ISE within which those investments must live and thrive.

Rather than dwell on the lack of impact of past IT investments, MOISA1 points out the need for community-centered design and implementation strategies that empower regional stakeholders to play key roles in directing the design of their future ISE. If we base future ISE initiatives on the ways people currently work and share information to accomplish their safety and security missions, these initiatives, whether IT-based or not, will sustain and grow, providing long-term benefits even beyond those for which they were initially intended.

A Acronyms

A

AIS	Automatic Identification System
ACE	Automated Commercial Environment
AMSC	Area Maritime Security Committees
ARES	Amateur Radio Emergency Service
ATS	Automated Targeting System

B

BAPLIE	Bayplan/stowageplan occupied and empty
BPM	Business Process Modeling
BPMN	Business Process Modeling Notation
BPMT	Business Process Modeling Toolkit

C

CART	Common Assessment Reporting Tool
CBP	Customs and Border Protection, Bureau of
CBP OAM	Customs and Border Protection Office of Air and Marine
CERT	Community Emergency Response Teams
CG1V	Coast Guard One View
CGBI	Coast Guard Business Intelligence
CINS	Cargo Incident Notification System and Organization
CNIC	Commander, Navy Installations Command
COARRI	COntainer ARRIval (EDI message)
COAC	Customs Operations Advising Committee
COP	Common Operational Picture
COPRAR	COntainer PRe-ARrival (EDI message)
CoSSaR	Collaborative Systems for Security, Safety and Regional Resilience
CORE	Common Operating and Response Environment
C-TPAT	Custom-Trade Partnership Against Terrorism
CVTS	Cooperative Vessel Traffic Service

D

DBSE	Document-Based Systems Engineering
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOD	Department of Defense
DOE	Department of Ecology
DOT	Department of Transportation

E

EDI	Electronic Information Exchange
EOC	Emergency Operating Center/Emergency Operations Center

F

FBI	Federal Bureau of Investigation
FCC	Federal Communications Committee
FEMA	Federal Emergency Management Agency
FSLTIPP	Federal, State, Local, Tribal, International, Public and Private

G

GAO	Government Accountability Office
GDP	Gross Domestic Product
GIS	Geographic Information System

H

HSIN	Homeland Security Information Network

I

IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
ILWU	International Longshore and Warehouse Union
IMO	International Maritime Organization
IOC	Interagency Operations Center
ISA	Importer Self-Assessment
ISA-IPC	Information Sharing and Access Interagency Policy Committee
IT	Information Technology
ITDS	International Trade Data System

J

JAC	Joint Analysis Center
JACIIS	Joint Analysis Collaboration Intel Infer System
JBLM	Joint-Base Lewis McChord
JHOC	Joint Harbor Operations Command

K	
KC	King County
L	
LLC	Limited Liability Company
LRIT	Long Range Identification and Tracking
M	
MARAD	Maritime Administration
MBSE	Model-Based Systems Engineering
MCOP	Maritime Common Operating Picture
MCTS	Marine Communications and Traffic Services
MDA	Maritime Domain Awareness
MISE	Maritime Information Sharing Environment
MISLE	Marine Information for Safety and Law Enforcement
MOA	Memorandum of Agreement
MOISA	Maritime Operations Information Sharing Analysis
MOU	Memorandum of Understanding
MSOC	Marine Security Operations Center
MTSA	Maritime Transportation Security Act
N	
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NMII	Naval Magazine Indian Island
NMIO	National Maritime Sharing Environment
NOAA	National Oceanic and Atmospheric Administration
NVAC	National Visualization and Analytics Center
NW WARN	NorthWest Warning, Alert & Response Network
O	
OEF	Operation Enduring Freedom
OEM	Office of Emergency Management
OIF	Operation Iraqi Freedom
OND	Operation New Dawn
OSHA	Occupational safety and health administration
OWF	Ozone Widget Framework
P	
PARVAC	Pacific Rim Visualization and Analytics Center
PGA	Participating Government Agencies
PM-ISE	Program Manager - Information Sharing Environment
PND	Ports for National Defense

PNNL	Pacific Northwest National Laboratory
PNWER	Pacific Northwest Economic Region
PSNS	Puget Sound Naval Shipyards

R

RIID	Radiation Isotope Identification Device
RO/RO	roll-on/roll-off
RPM	Radiation Portal Monitor

S

SAFE Port	Security and Accountability for Every Port
SAR	Search and Rescue
SAWC	Situational Awareness and Watch Center
SCAC	Standard Carrier Alpha Code
SIIS	Statewide Integrated Intelligence System
SPD	Seattle Police Department
SPOC	Seattle Police Operations Center
SRS	System Requirements Specification

T

TCW	Trust Company of the West
TEU	Twenty-Foot Equivalents
TWIC	Transportation Worker Identification Credential

U

UML	Unified Modeling Language
USACE	United States Army Corps of Engineers
USCG	U.S. Coast Guard
USDA	United States Department of Agriculture
UW	University of Washington

V

VACIS	Vehicle and Container Inspection System
VTS	Vessel Traffic System

W

WANG	Washington National Guard
WCO	World Customs Organization
WDFW	Washington Department of Fish and Wildlife
WEB EOC	Web Emergency Operations Center
WSDOT	Washington State Department of Transportation
WSFC	Washington State Fusion Center
WSP	Washington State Patrol

B Glossary

B

BAPLIE A message to transmit information about equipment and goods on a means of transport, including their location on the means of transport. The message can be exchanged between (liner's) agents, tonnage centers, stevedores and ships masters/operators.

C

COARRI A message by which the container terminal reports that the containers specified have been discharged from a seagoing vessel (discharged as ordered, overlanded or shortlanded), or have been loaded into a seagoing vessel.

COPRAR A message to order to the container terminal that the containers specified have to be discharged from a seagoing vessel or have to be loaded into a seagoing vessel. This message is part of a total set of container-related messages. These messages serve to facilitate the intermodal handling of containers by streamlining the information exchange.

Common Operating Picture A common operating picture is established and maintained by gathering, collating, synthesizing, and disseminating incident information to all appropriate parties. Achieving a common operating picture allows on-scene and off-scene personnel — such as those at the Incident Command Post, Emergency Operations Center , or within a Multiagency Coordination Group — to have the same information about the incident, including the availability and location of resources and the status of assistance requests.

E

EDI An electronic data interchange (EDI) is the transmission, in a standard syntax, of unambiguous information of business or strategic significance between computers of independent organizations.

EDI 309 The transaction set can be used by carriers, terminal operators, port authorities, or service centers to provide Customs with manifest data on cargo arriving in or departing from oceangoing vessels, railroad trains, or other types of conveyances. The transaction set can also be used by carriers to provide terminal operators, port authorities, or service centers with manifest data on cargo arriving at their facilities via the conveyances mentioned above.

EDI 322 The transaction set can be used to provide all the information necessary for a terminal operation, port authority or intermodal ramp to communicate terminal and intermodal ramp activities to authorized parties to a shipment.

EDI 350 The transaction set can be used by the Customs Service (CS) to supply carriers, terminal operators, port authorities, and service providers with cargo release and cargo hold information for import shipments. It can also be used by the CS to provide exporters or their agents, carriers, and service providers with information pertaining to export shipments.

Express Express is a comprehensive terminal information management product... Express handles a complete range of terminal business transactions such as import and export processing, bookings, gate activity, equipment management, billing, EDI (electronic data interchange), and more.

Equipment Interchange Receipt A document required when transferring a cargo container from one vessel to another, or to a shipping terminal.

F

FSLTIPP Federal, state, local, tribal, international, public, and private entities. "Public sector" and "private sector" are economic terms. "Federal", "state", "local," and "tribal" refer to government entities. Therefore, it appears that the term FSLTIPP is a composite of terms meant to differentiate different forms of government entities and economic arrangements.

I

Interoperability Interoperability describes the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user.

IT System A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. An interconnected set of information resources under the same direct management control, which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. Refers to a set of information resources under the same management control that share common functionality and require the same level of security controls.

M

Model A model is an approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system.

S

SCAC The Standard Carrier Alpha Code is assigned by the National Motor Freight Traffic Association as a unique identifier for motor carriers.
Scenario A scenario is a sequence of actions that illustrates behavior and appears within a use case model as a single thread or pathway through the use-case.

T

Thematic Analysis A qualitative analytic method for identifying, analyzing, and reporting patterns (themes) within data. It minimally organizes and describes your data set in (rich) detail. However, frequently it goes further than this, and interprets various aspects of the research topic.

U

Use-Case A use-case is a prose or (graphical) description of a system's behavior when interacting with the outside world. A use-case is comprised of scenarios.

C Phase 1 Formal Interviews

- Amateur Radio Emergency Service (ARES)
- APM Terminals B.V. (LLC) - Commercial Operations at Port of Tacoma
- Bainbridge Island Police Department
- Canadian Coast Guard Marine Communications and Traffic Services (MCTS), IT
- Canadian Coast Guard Marine Communications and Traffic Services (MCTS), Pacific Region, Operations
- Canadian Coast Guard Marine Communications and Traffic Services (MCTS) Western Region (Victoria, Canada)
- Canadian Coast Guard Marine Security Operations Center (MSOC)
- City of Everett Emergency Operations and Fire Department
- City of Seattle Office of Emergency Management (OEM)
- Customs and Border Patrol (CBP) Office of Air and Marine
- Department of Natural Resources (DNR]
- Federal Emergency Management Agency (FEMA), Federal Regional Center
- Federal Emergency Management Agency (FEMA), Response
- Gleaves Consulting
- Joint Harbor Operations Center (JHOC)
- King County Emergency Management
- King County Sheriff Air Support Unit
- King County Sheriff Marine Rescue and Dive Unit

- Kitsap County Emergency Management Office
- National Oceanic and Atmospheric Administration (NOAA)
- Naval Base Kitsap-Bangor
- Pacific Merchant Shipping Association (PMSA)
- Pacific Northwest Economic Region (PNWER)
- Pacific Northwest National Laboratory (PNNL)
- Pierce County Department of Emergency Management
- Port Gamble South S'Klallam Tribe
- Port of Everett
- Port of Olympia
- Port of Seattle, Seaport Security
- Port of Tacoma
- Puget Sound Pilots
- Puyallup Tribal Police Department
- Search and Rescue (SAR) at Canadian Coast Guard Marine Communications and Traffic Services (MCTS)
- Seattle Fire Department
- Seattle Police Department (SPD)
- Seattle Police Operations Center (SPOC)
- Snohomish County Sheriff's Office
- Takouba Security
- Tribe Police/Fish and Wildlife
- U.S. Coast Guard Auxiliary
- U.S. Coast Guard (USCG), Contingency Planning
- U.S. Coast Guard (USCG), District 13
- U.S. Coast Guard (USCG) Electronic Support Unit
- U.S. Coast Guard (CG), Prevention
- U.S. Coast Guard (CG), Response
- Valley Communications Center

- Washington State Ferries
- Washington State Fish and Wildlife Enforcement (WDFW)
- Washington State Fusion Center (WSFC)
- Washington State Patrol (WSP)
- West Pierce Fire and Rescue
- Western Towboat Co.

D Phase 1 Interview Protocol

- Basic information
- Interviewee job role & work context
  - Recurring events/example scenarios
- Information sharing
  - Who do you depend on/who depends on you? (Within/external to organization)
  - Types of information needed/shared
    - Source
    - Trigger
    - Purpose
    - Used by
    - Mode of sharing (*e.g.*, email, Twitter, formal/informal)
    - Difficulty of sharing (degree and reason for difficulty)
  - Information gaps and barriers, challenges to getting/sharing needed info
  - Impact of regulation and policy
  - Agreements and MOUs
- Information resources
  - Type, shared by, extent of control, adequacy
  - Social media
  - IT contact?
- Rad/Nuke
- Values and culture
  - Impact of leadership structure on info sharing

1. Does your organization use radiological detection equipment in day-to-day operations? □ Yes □ No

   (a) If no - should it? □ Yes □ No

2. Is radiation/nuclear (rad/nuke) alarm adjudication part of your mission? □ Yes □ No

   (a) If yes - does your organization have the equipment capability, protocols and appropriate training to conduct that adjudication? □ Yes □ No

3. Is your organization equipped (personnel, training, equipment, procedures) for sharing and/or communicating radiation/nuclear (rad/nuke) alarm or event information? □ Yes □ No

E Phase 1 Codes

- MOUs
  - Non-specified agreements
  - No agreements/MOU/MAA
- DNDO
- DNDO not mentioned
- Policy and regulation
- Successful or non-problematic share
- Information sharing
  - Difficulty of sharing
    - Non-ICT difficulty
      - A huge need For privacy
      - Differing perceptions/disconnect between workflow and information flow
      - Clearance/policy
      - Organizational culture
      - Ambiguity
    - Both ICT and non-ICT difficulty
    - ICT difficulty
  - Both ICT and non-ICT
  - ICT non-difficulty
  - Non-ICT non-difficulty
- Informal work
- Information
  - Reports
- Crossover functionality

- Collaboration
  - Collaboration difficulty
- Relationships
- Land-maritime split
- Commercial cargo
- Degree of difficulty
  - Not a problem
  - Nice to have
  - Bottleneck
  - Barrier
  - Degree of difficulty not specified
- Solution/workaround
  - Hypothetical Solution
  - Actual solution
- Bottom up information flow
- Modes
  - Radio
  - Email
  - Phone
  - Face-to-face
    - Meetings
  - Mode not specified
  - Other Modes
    - QR codes
    - Business cards
    - Lights
    - Text
    - Paper
    - News media
    - Video
    - Cameras/images
    - Air card
    - Alerts/siren/alarm/warning

  - Information system
  - Public web-based resources
    - Social media
    - Does not use social media
    - No social media reference
- Mode pivot
- Reciprocity
- Experience
  - Job turnover
- Resource alignment
  - Difficulty resource alignment
  - Competition
- Props and praise
- Trust
  - Length of relationship
- Attributes specific to content
  - Timeliness
  - Credibility
  - Utility/usefulness
- Sharing partner
  - Public
  - Bettie
  - Role
  - Organization
  - Leadership
  - Authority
  - Control
  - Background knowledge
  - Interoperability
  - Access
  - Need to know
  - Permission
  - Clearance

F Abridged Systems Analysis

System	Used by	Tags	Tags self-defined or standard?	ID management	Federal funding
Email	Everyone	None	N/A	PW	
ARC GIS	Most on the water	N/A	N/A	N/A	
Blue Force Tracker	Most with boats	N/A	N/A	N/A	
CommandBridge	SPD, SFD, USCG	Access	Self-defined	PW	PSGP
CORE	CBP, PNNL, DNDO, JAC	Access, Discovery	Self-defined	PW, factor IP	
DEM Portal	Pierce County	N/A	N/A	N/A	
DNDO Website	DNDO, SFD	N/A	N/A	N/A	
FirstToSee	Pierce County EOC, PNWER	None	N/A	PW	PSGP
I/LEADS	Bainbridge Island PD				
IWIN	CBP				
Kronos Telestaff	Port of Tacoma	None	N/A	PW	
LEARN	Bainbridge Island PD				
MCOP	SPD, SFD, USCG	None	N/A		PSGP
NIXIE	Bainbridge Island PD	None	N/A	PW	
NW WARN	Everett EOC, Snohomish Sheriff, PNWER	N/A	N/A	N/A	
OSKAR	Bainbridge Island PD				
PCWARN	Pierce County	N/A	N/A	N/A	
PCALERT	Pierce County	N/A	N/A	N/A	
PIER	Port of Everett	Access, Discovery	Self-defined	PW	
Pierce County Intranet	Pierce County	None	N/A	PW	
Port of Everett Sharepoint	Port of Everett	Discovery	Self-defined	PW	
Search Engine	SFD				
Seattle FD Sharepoint	SFD	Yes	Self-defined		
SIGNALIS	Canada CG				
ViewPointe	SPD, SFD, EMT, Federal				PSGP
Spillman	Skagit County, Island County, San Juan	Yes	Spillman standard	PW	PSGP
Wildcomm	WDFW				
WebEOC	Pierce County	None	N/A		Various grants
PremierOne	WSP	Access, Discovery	Motorola standard		

G DNDO Summary

Summary of Answers		**N = 47**	**%**
1. Does your organization use radiological detection equipment in day-to-day operations?			
	Yes	14	30
	No	22	47
	Not Documented	11	23
1a. If no, should it?		(N = 22)	
	Yes	3	14
	No	14	64
	Indeterminate	3	14
	Not Documented	2	9
2. Is radiation/nuclear (rad/nuc) alarm adjudication part of your mission?			
	Yes	12	26
	No	20	43
	Not Documented	15	32
2a. If yes, does your organization have the equipment capability, protocols and appropriate training to conduct that adjudication?		(N = 12)	
	Yes	8	67
	No	3	25
	Indeterminate	1	8
3. Is your organization equipped (personnel, training, equipment, procedures) for sharing and/or communicating radiation/nuclear alarm or event information?			
	Yes	17	36
	No	9	19
	Indeterminate	2	4
	Not Documented	19	40

G.1 Narrative Summary of Quantitative Results

- Of the 47 units in our sample, 14 interviewees reported using radiation/nuclear detection equipment in their day-to-day operations.
- Of the 14 interviewees that reported using radiation/nuclear detection equipment in their day-to-day operations, 12 interviewees see radiation/nuclear alarm adjudication as part of their mission. Of these 12, 3 interviewees reported that their organization does not have the equipment capability, protocols, and appropriate training to completely conduct that adjudication. Specifically: An interviewee form U.S. Coast Guard (USCG), Sector Puget Sound Contingency Planning stated that the USCG does not have the training to do this well. Another interviewee in USCG Response reported that Level 1 detectors are fine, but although their personnel receive Level 2 (identifying the threat) training, they do not use Level 2 training often enough to remain proficient.
- 22 interviewees reported that using radiation/nuclear detection equipment is not part of their day-to-day operations; of these 22 entities, 3 reported believing that it should be:
  - 2 of these are tribal entities: (1) the Puyallup Tribal Police, and the (2) Tullalip Tribal Police/Fish and Wildlife Enforcement, (2) Indicated that if they had the equipment, they could communicate alarm information to USCG.
  - King County Sheriff, Aviation wants the use of radiation/nuclear detection equipment to be included in their mission because they are often the first people on the scene and they currently have to wait for someone who has the equipment to arrive.
- 9 interviewees reported that their organization is not equipped for sharing and/or communicating radiation/nuclear alarm event information.

G.2 Summary of Qualitative Discoveries

The following is a summary of the most salient themes that emerged in a subset of 21 interviews and observation and participation in two radiation/nuclear exercises facilitated by PNNL.

G.2.1 Land/Maritime Split

- Different, yet overlapping processes for handling land- vs. water-based threats creates confusion for agencies that handle both (*e.g.*, Seattle Fire Department).

- The perceived lack of a single coordinating entity for land-based threats makes handling land-based threats more difficult than handling threats on the water.

- There is a perception that there are more resources and equipment for handling land-based threats than threats on the water.

- The distinction between land and water is false, as resolving threats on the water necessitates coordination with entities that do not have a maritime focus.

G.2.2 Different Systems for Reach Back

- There are three different systems for reach back and analysis in use in the region: CORE for maritime incidents, JACCIS for land-based incidents and Triage, which is used for both.

- Managing multiple authentication processes for multiple systems is challenging and time consuming, even under benign training conditions.

- Individuals have personal preferences for working with specific labs based on a perception that scientists at different labs have different training.

- Loyalty to specific labs is based on relationships established prior to 911.

G.2.3 Funding and Attendance

- Funding a regional radiation/nuclear program with Port Security Grant Program funds may negatively impact continuity of the program.

- PSGP funding restrictions on payment of overtime to federal employees may hinder participation.

- Funding and staffing issues are barriers to smaller entities' participation.

G.2.4 Illuminating Available Resources

- By attending the exercises, participants gain visibility into the existence and availability of resources (personnel and equipment) of neighboring entities.

G.3 Narrative Summary of Qualitative Discoveries

G.3.1 Land/maritime Split

From the perspective of someone from the Department of Health's Radiological Emergency Preparedness Section, managing radiation/nuclear threats on the water is much simpler than managing these threats on land because maritime entities have one coordinating facility-the JHOC-via which all information flows. This was later expanded on by a member of the State Office of Radiation Protection who stated that the biggest difference between water and land events is the Captain of the Port. According to the DOH, they are still in the process of trying to identify a coordinating entity on land, and although some believed that the Fusion Center would be this entity, it is not currently ready or "set up" to perform this role.

We received differing reports as to whether and how the connections between land and maritime will occur in the case of an event. JHOC indicated they would contact FBI, 10th Civil Support Team (CST) and the WSP bomb squad. The WSP bomb squad would secure the area and look for the threat. Next a RAP (Radiological Systems Program) team would come out after FBI or LSS contacts them. A RAP team usually participates in the regional radiation/nuclear exercises.

An interviewee from the Seattle Fire Department (SFD) stated that there are different policies that govern the way radiation/nuclear threats are handled on land than on water. He indicated that there is some overlap in the way things are handled on land and water, which 'should make it easier,' however, he wonders why "... we need to invent a brand new way to do things when the equipment is the same." According to the interviewee, land has more resources for radiation/nuclear detection than water and reachback is more difficult on the water than it is on land.

Our USCG liaison pointed out that in one sense the land/maritime split is an illusion-as soon as anyone on the maritime side finds and adjudicates a threat, they then have to pass it off to someone on land, yet land based entities that would be a part of the handoff are conspicuously absent at maritime exercises, in fact they may not even have received an invitation.

G.3.2 Local Role of Seattle Fire Department (SFD)

The Seattle Fire Department plays an important role in the local radiation/nuclear detection scene. They are working towards standardizing equipment in the area and a State equipment standardization committee is chaired by an SFD Chief. The Seattle Fire Department has a great variety of radiation/nuclear resources that are part of a Port Security Grant funded program. SFD is required to use Custom and Border Patrol's (CBP) Laboratories and Scientific Services (LSS) to get an analysis of the nature of the threat, in part because LSS then shares this information with the Federal Government. However, SFD feels that they could perform the analysis more quickly and just as well themselves.

G.3.3 Different Systems for Reach Back

In addition to SFD, a number of other interviewees expressed skepticism about the requirement to use LSS. CBP owns LSS and will only send their data through LSS for analysis because, they say, LSS scientists have different and better training. However, interviewees from PNNL who have visited LSS and other labs say that the procedures do not differ. When asked why there are so many labs, one person from PNNL said "I don't know. . . " Another interviewee commented that CBP only uses LSS because that is who always analyzed their data before Customs was split into three post-911 entities under DHS.

For maritime exercises, PNNL uses CORE to do reach back for threat identification. CORE was developed specifically for and is used exclusively by the Puget Sound region. It was designed to address a gap in different entities' ability to share information with one another. It is a Web-based system to which all agencies should have access, however 2-step authentication and the relative rarity of people needing to log into the system makes accessing the system time consuming. The second authentication factor relies on a printed matrix of codes from which the user must enter the correct code. Our observation of the effort while underway on one of the response boats indicated that this was a challenge even under benign training conditions.

CORE is said to be different from other reporting systems in that it enables first responders to add situational awareness data, *e.g.*, who's on scene, where they are, who they are encountering. First responders can also upload photos of the layout, which is particularly helpful for responders who are on their way to the scene, because they can review and plan in advance. For land incidents, units use the Joint Analysis Center Collaborative Information System (JACCIS), which also has a specific situational awareness component. The JACCIS is viewed as a one-stop place for land-based events, but JHOC remains the hub for maritime exercises and incidents. There is also the NNSA Triage system, which everyone in the country uses, however, Triage only handles spectra data-not situational awareness.

G.3.4 Funding and Attendance

Grant funding is not the best mode of supporting a regional radiation/nuclear program because starts and stops in the cash flow cause the regional team to lose ground. Also, the amount of money and restrictions on how it can be spent change every year, making it difficult to plan the program ahead of time. There is a perception that were it not for the outside grant funding, agencies would not participate in radiation/nuclear detection activities at the same level of commitment as they do with the grant funding.

At one of the exercises, a glance at the attendance roster revealed that almost half of the exercise attendees, including those from USCG and CBP, had noted that they were in "overtime" status. However, since the exercise was funded through a Port Security grant, payment to federal employees is restricted. Clearly there are potentially detrimental tensions between funding a radiation/nuclear program through the PSGP, and the full participation of federal employees who would play key roles in the event of an actual incident.

PNNL is aware of a handful of agencies that don't attend the exercises but wish they could. PNNL suspects that they do not attend because they can't afford to financially or because they can't spare the person power. This primarily impacts smaller entities with few staff. For example, the Suquamish Tribal Enforcement entities have only three officers to patrol a very wide area, and they need to prioritize having people on patrol rather than attending exercises. An additional reason that some entities don't attend is because some supervisors "don't support the mission." As one interviewee from PNNL put it, "Budgets are making it harder to include new agencies."

G.3.5 Illuminating Available Resources

One of the important outcomes of radiation/nuclear exercises is to illuminate the availability of needed resources. At one of the exercises, one of the facilitators from PNNL stated that the FBI was expected to attend and bring their resources, and that these resources included a boat and possibly some detection equipment, but that the FBI had canceled their attendance with little warning. The facilitator explained that this would not be a problem because an officer from Bainbridge Island Police Department (BIPD) would bring BIPD resources and thereby fill the resource gap left by the FBI. While the lack of FBI participation was a lost opportunity for building community and getting to know others who FBI would need to work with in the event of an actual incident, attendees learned that BIPD could be called on to provide resources in the event the FBI could not. Thus the exercise provided visibility into the existence of local resources of which attendees might not otherwise be aware. (Note: a subsequent interviewee questioned whether FBI resources would include a boat.)

Entities Represented in the Sample

- Amateur Radio Emergency Services (ARES)
- APM Terminal at Port of Tacoma
- Bainbridge Island Police Department
- City of Everett Emergency Operations and Fire Department
- City of Seattle Emergency Operations Center
- Customs and Border Patrol (CBP)
- King County Sherriff, Aviation
- King County Sherriff, Marine
- Marine Security Operations Centre (MSOC)
- Navy, Bangor Naval Base
- National Oceanic and Atmospheric Administration
- Pierce County Emergency Management
- Pacific Northwest Economic Region (PNWER)
- Port Gamble S'Klallam Tribe
- Port of Everett, Security
- Port of Olympia, Security
- Port of Seattle, Seaport Security
- Port of Tacoma, Security
- Puget Sound Pilots Association
- Puyallup Tribal Police
- Seattle Fire Department
- Seattle Fire Department
- Seattle Police Department
- Snohomish County Sherriff's Office

- Seattle Police Department, Operations
- TullalipTribal Police/Fish and Wildlife
- U.S. Coast Guard, Contingency Planning
- U.S. Coast Guard, Electronic Support Unit Contractor
- U.S. Coast Guard, Prevention
- U.S. Coast Guard, Response
- U.S. Coast Guard, Auxiliary
- Valley Communications 911 Call Center
- Victoria, Canada Coast Guard
- Washington State Ferries
- Washington State Fish and Wildlife Enforcement
- Washington State Department of Natural Resources
- Washington State Emergency Management Division
- Washington State Fusion Center
- West Pierce Fire
- Western Tow

H Phase 3 Information Dictionary

- BAPLIE:
  - Terminal managers discuss plans; input Ocean Carrier Email.BAPLIE
- bookingNumber:
  - Main gate procedure; input Trucker.bookingNumber
  - Ocean carrier initiates transport to CES; output Ocean Carrier Email.bookingNumber
  - Conduct main gate procedures; input Trucker.bookingNumber
  - Obtain ticket; output TIR.bookingNumber
- CESlocation:
  - Ocean carrier initiates transport to CES output; Ocean Carrier Email.CESlocation
- chassisNumber:
  - Verify transaction; input Trucker.chassisNumber
- clerkInstructions:
  - Trucker calls longshore clerk to discuss load; output Clerk.clerkInstructions
- COARRI:
  - Unload container; output SPARCS.COARRI
- containerID:
  - Scan container; input handheldComputer.containerID
  - Main gate procedure; input Trucker.containerID
  - Ocean carrier initiates transport to CES output; Ocean Carrier Email.containerID
  - Conduct main gate procedures; input Trucker.containerID
  - Obtain ticket; output TIR.containerID
  - Verify transaction; input Trucker.containerID

- containerImage:
  - CBP drive by scan; output VACIS.containerImage
- containerLocation:
  - Move container to resting place; input EXPRESS.containerLocation
  - Move container to resting place; output EXPRESS.containerLocation
  - Unload container; input SPARCS.containerLocation
  - Terminal determine if and where container needs to be moved; input EXPRESS.containerLocation
  - Terminal determine if and where container needs to be moved; output EXPRESS.containerLocation
  - Terminal moves container to inspection location; input EXPRESS.containerLocation
  - Terminal moves container to inspection location; output EXPRESS.containerLocation
  - Terminal moves contaminated container to frustrate yard; input EXPRESS.containerLocation
  - Terminal moves contaminated container to frustrate yard; output EXPRESS.containerLocation
  - Terminal obtains weight receipt; output EXPRESS.containerLocation
  - Terminal weighs cargo; output EXPRESS.containerLocation
  - Drop off container; input TIR.containerLocation
  - Obtain ticket; output TIR.containerLocation
  - Pick up container; input TIR.containerLocation
- containerSize:
  - Obtain ticket; output TIR.containerSize
- containerWeight:
  - Obtain ticket; output TIR.containerWeight
- contaminantType:
  - CBP agricultural officer inspects container for contaminant; output CBP Inspector.contaminantType
  - Terminal determine if and where container needs to be moved; input CBP Inspector.contaminantType
- COPRAR:
  - Unload container; input SPARCS.COPRAR

- crewManifest:
  - Review personnel information; input Captain's email.crewManifest
- customsForm6043:
  - Main gate procedure; input Trucker.customsForm6043
- date:
  - Obtain ticket; output TIR.date
- dispositionPlan:
  - Terminal managers discuss plans; input Operations Manager.dispositionPlan
- eDI309:
  - CBP drive by scan; input ACE.eDI309
  - CET inspection; input ACE.eDI309
  - CBP agricultural officer inspects container for contaminant; input ACE.eDI309
  - CBP agricultural officer reinspects container ;input ACE.eDI309
  - CBP secondary inspection (RIID); input ACE.eDI309
- eDI322:
  - Scan container; output EXPRESS.eDI322
  - Scan container; output SPARCS.eDI322
  - Main gate procedure; output EXPRESS.eDI322
  - Main gate procedure; output Notify Party EDI System.eDI322
  - Main gate procedure; output ACE.eDI322
  - Conduct main gate procedures; output EXPRESS.eDI322
  - Conduct main gate procedures; output Notify Party EDI System.eDI322
  - Verify transaction; output EXPRESS.eDI322
  - Verify transaction; output Notify Party EDI System.eDI322
- eDI350:
  - CBP drive by scan; input ACE.eDI350
  - CBP drive by scan; output ACE.eDI350
  - CBP drive by scan; output EXPRESS.eDI350
  - CET inspection; input ACE.eDI350
  - CET inspection; output ACE.eDI350

  - Ocean carrier initiates transport to CES; input ACE.eDI350
  - CBP agricultural officer inspects container for contaminant; input ACE.eDI350
  - CBP agricultural officer inspects container for contaminant; output ACE.eDI350
  - CBP agricultural officer reinspects container; input ACE.eDI350
  - CBP agricultural officer reinspects container ;output ACE.eDI350
  - CBP secondary inspection (RIID); input ACE.eDI350
  - CBP secondary inspection (RIID); output ACE.eDI350
  - Electronially clear container for intermodal transport; input ACE.eDI350
  - Electronially clear container for intermodal transport; output EXPRESS.eDI350
  - Terminal determine if and where container needs to be moved; input ACE.eDI350
  - Terminal moves contaminated container to frustrate yard; input ACE.eDI350

- EIR:
  - Verify transaction; output EXPRESS.EIR

- equipmentIssues:
  - Terminal managers discuss plans; input Maintenance and Repair Manager.equipmentIssues

- guardPlan :
  - Finalize draft plans input; Security plan.guardPlan
  - Finalize draft plans output; Security plan.guardPlan
  - Revise pro forma guard plan 0; output Security plan.guardPlan

- hazardousPlacards:
  - Terminal checks hazardous placards; input Truck .hazardousPlacards
  - Terminal checks hazardous placards; input OCR Scanner.hazardousPlacards

- importAlert:
  - CBP secondary inspection (RIID); input ATS.importAlert

- inspectionNoPass:
  - CBP agricultural officer inspects container for contaminant; output CBP Inspector Email.inspectionNoPass

- Terminal moves contaminated container to frustrate yard; input CBP Inspector Email.inspectionNoPass

- inspectionOrder:

  - Terminal managers discuss plans; input CBP Email.inspectionOrder

- loadStatus:

  - Trucker calls longshore clerk to discuss load; input Trucker.loadStatus

- loadWeight:

  - Terminal weighs cargo; output scale.loadWeight

- loadWeightReceipt:

  - Terminal obtains weight receipt; input Trucker.loadWeightReceipt

- longshoremanSchedule:

  - Terminal managers discuss plans; input Operations Manager.longshoremanSchedu

- outOfGaugeCargo:

  - Terminal managers discuss plans; input Ocean Carrier Email.outOfGaugeCargo

- passengerManifest:

  - Review personnel information; input Captain's email.passengerManifest

- planChange:

  - Terminal managers discuss plans; input Security plan.planChange
  - Terminal managers discuss plans; output Security plan.planChange

- portOfDischarge:

  - Obtain ticket; output TIR.portOfDischarge

- Radiation guage:

  - CBP secondary inspection (RIID;) input Handheld RIID.Radiation guage

- radtionanAlarm:

  - CBP secondary inspection (RIID); input PRD.radtionanAlarm

- scacCode:

  - Main gate procedure; input Trucker.scacCode
  - Conduct main gate procedures; input Trucker.scacCode

- sealNumber:

  - Conduct main gate procedures; input Trucker.sealNumber

- shipHusbandrySchedule:
  - Review vessel schedule; input Shipping Agent.shipHusbandrySchedule
- shuttlePlan:
  - Add escort or shuttle plan; output Security plan.shuttlePlan
  - Finalize draft plans; input Security plan.shuttlePlan
  - Finalize draft plans; output Security plan.shuttlePlan
- shuttleRequest:
  - Review personnel information; input Captain's email.shuttleRequest
- steamCleaningReceipt:
  - CBP agricultural officer reinspects container; input Steam Cleaning Company.steamCleaningReceipt
  - Certified company steam cleans contaminated container; output Steam Cleaning Company.steamCleaningReceipt
- steamCleanOrder:
  - Certified company steam cleans contaminated container; input Terminal.steamCleanOrder
  - Terminal moves contaminated container to frustrate yard; output Terminal.steamCleanOrder
- time:
  - Obtain ticket; output TIR.time
- TIR:
  - Verify transaction; input Trucker.TIR
- tractorChassisWeight:
  - Conduct main gate procedures; input Trucker.tractorChassisWeight
- truckCompanyName:
  - Conduct main gate procedures; input Trucker.truckCompanyName
  - Obtain ticket; output TIR.truckCompanyName
- TWICstatus:
  - Check security status; input Trucker.TWICstatus
- unloadingPlan:

  - Unload container; input SPARCS.unloadingPlan
  - Terminal managers discuss plans; input Operations Manager.unloadingPlan

- vacisAlarm:
  - CBP secondary inspection (RIID); input VACIS.vacisAlarm
- VACISlist:
  - CBP drive by scan; input CBP Email.VACISlist
- vendorList:
  - Review personnel information; input Port Engineer's email.vendorList
- vesselName:
  - Obtain ticket; output TIR.vesselName
- vesselSchedule:
  - Terminal managers discuss plans; input Operations Manager.vesselSchedule
  - Review vessel schedule; input Operations Manager.vesselSchedule
- visitorList:
  - Review personnel information; input Captain's email.visitorList