


MOISA 2:

Fostering Regional Partnerships and Innovation for Maritime Security, Safety, and Resilience

September 2015
Version 1.1

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

First printing, September 2015

TITLE PAGE IMAGES

US Coast Guard photo by Petty Officer 3rd Class Nathan Bradshaw. (2012). "Petty Officer 1st Class Ramona Mason, an operations specialist and VTS Puget Sound watchstander, monitors vessel traffic in the Strait of Juan de Fuca." http://coastguard.dodlive.mil/2012/10/40-years-of-safe-navigation-in-americas-waterways/#sthash.7cVlSTwF.dpuf

King County Sheriff's Office. (no date). http://www.kingcounty.gov/safety/sheriff/Enforcement/Specialized/MarinePatrol.aspx

USCG. (2014). "Air Station/ Sector Field Office (SFO) Port Angeles, WA." http://www.uscg.mil/d13/sfoportangeles/Photo_Gallery/

Version Control

Table 1: *Table of Changes*

Version	Effective Date	Approved By	Change
1.0	9/30/2015	Mark Haselkorn	Initial Report
1.1	1/27/2016	Mark Haselkorn	Minor amendments to verbiage

Acknowledgements

The University of Washington acknowledges the contributions made to the research and publication of the MOISA Year 2 Report. We would like to thank the Puget Sound maritime community for their participation. Specifically, we thank the:

- Air Station/Sector Field Office (SFO) - Port Angeles, WA
- APM Terminals
- Area Maritime Security Committee – Puget Sound
- Canadian Coast Guard
- Clallam County Sheriff
- Customs and Border Protection – Border Patrol - Blaine, WA
- Customs and Border Protection – Office of Air and Marine – Bellingham, WA
- Coupeville Marshal's Office
- Drug Enforcement Agency
- East Jefferson Fire Rescue
- Homeland Security Division for Washington State Patrol
- Jefferson County Sheriff
- King County Sheriff
- King County Sheriff's Aviation Support Unit
- Marine Exchange of Puget Sound
- Northwest Maritime Center
- Pierce County Sheriff's Office
- Pierce County Emergency Management
- Port of Everett
- Port of Tacoma
- Puget Sound Area Maritime Security Committee
- Puget Sound Marine Exchange
- Royal Canadian Mounted Police
- Skagit County Sheriff
- Snohomish County Sheriff
- USCG District Thirteen
- USCG Sector Puget Sound
- USCG Station Seattle
- US Drug Enforcement Agency – Seattle, WA
- Washington State Department of Fish and Wildlife
- Washington State Fusion Center
- Washington State Patrol
- Western Air Defense Sector
- Whatcom County Sheriff

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

Graduate Students: Melissa Braxton and Maura Rowell

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

UW Staff: Chris Hussein, Elizabeth Kirby, Sonia Savelli, and Brian Zito (LCDR, USN Retired)

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

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report of the second year of the Maritime Operational Information Sharing Analysis project (MOISA 2) provides new information, analysis, development activity, strategic approaches, and demonstrations that build on the promise of MOISA 1 to help foster regional partnerships and innovation for regional security, safety, and resilience. The focus of these partnerships and innovations is on achieving mission relevant enhancements to the regional information sharing environment (ISE). MOISA 2 produced many valuable products (outlined below), but its primary contribution is the articulation and demonstration of a repeatable, evidence-based, human centered process for integrating the full range of port partners into the design, development, and fielding of system enhancements to the regional ISE.

Section 4 reports on two related products that fed into the ISE partnering and information enhancement effort: (1) the first iteration of a regional sensor survey, and (2) the outcomes of community workshops that analyzed opportunities for enhanced mission accomplishment through increased sensor sharing. These efforts explored the potential of increased sharing of sensor and other regional data to enhance mission accomplishment. The workshops uncovered important opportunities, as well as difficult challenges to address if those opportunities were to be realized. Key takeaways such as the increased importance of mobile sensors, the desire for increased transparency of capabilities, and the interest in collaboratively tracking small vessels through different areas of responsibility hold important implications for future collaborative technology innovation such as a regional enterprise architecture. On the other hand, the workshop articulated challenges such as the burden of widespread information sharing during daily operations, the need for brokered agreements among diverse stakeholders, and the need for local control of accessibility to shared information.

Section 5 reviews the current regional technological context for ISE innovation, with particular focus on the DHS S&T project to demonstrate a regional enterprise architecture, known as IMDE/CSS. In addition, this section explores other regional collaborative systems currently in use and their relationship to the IMDE/CSS pilot effort. Particular attention is paid to:

- *Spillman*: a commercial product that began as a law enforcement software program to manage records and information electronically and has evolved to include 48 integrated modules that support such tasks as records management (RMS), computer-aided dispatch (CAD), mobile data and field reporting, mapping and GIS.
- *CommandBridge*: a commercial product that provides situation management collaboration and coordination to the maritime community. In the Puget Sound, CommandBridge is the situational awareness component of the Washington Common Operating Platform (WA-COP), a secure, collaborative software platform developed under Port Security Grant funding to support information sharing and decision making for public and private maritime and related stakeholders.
- HSIN: a DHS service that provides a SharePoint web portal system that allows Federal and non-Federal agency partners to share "Sensitive But Unclassified (SBU)" data over a secure channel. HSIN supports real-time communications for emerging threats and incident response and to help intelligence analysts and public safety officials across the country to share information.

In light of the planned IMDE/CSS demonstration, this section analyzes both opportunities for and constraints to technology innovation in support of ISE enhancements, particularly related to the introduction of a regional enterprise architecture.

Section 6 explores and analyzes two critical use cases of the regional security, safety and resilience community: (1) suspicious small vessel security activities and (2) operational planning and scheduling. The examination of small vessel security presents the business processes, technology, and environment of partners in local waters near the Canadian border in their detection, tracking and recognition of suspicious small vessels. The focus is on the local partners, which brings important new perspective on what is usually viewed as a Federal activity. This in turn raises the possibility of enhanced small vessel security through a more collaborative regional effort. While any efforts to move in this direction must recognize that safety is the overwhelming current local driver of maritime small vessel activity, the general recognition of a potential security threat posed by small suspicious vessels is clear. This is

evidenced in current federal/local joint patrols and general interest in improved awareness of the location of friendly (blue) assets.

For the second use case, MOISA 2 researchers articulated planning and scheduling activates that focus on daily operations and encompass both single-agency and inter-agency operations. This sub-section not only describes the current state of planning and scheduling for our interviewees, but also aided us in scoping the use case for a series of human-centered, iterative design and development cycles of an IMDE/CSS planning and scheduling module, described in the following section. Among other results, we found that current planning and scheduling processes require planners to spend considerable time and effort manually integrating information from a variety of information resources; that agencies have limited visibility into one another's current operations and even less into their future plans; that the specificity of plan and schedule documentation varies by agency and mission type (interagency vs. single agency); that agencies have different concepts of planning and scheduling tasks and resources; and that common core information attributes transcend the boundary between pre-planned and emergent events. This sub-section also begins a discussion of strategic approaches to challenges to integrating regional operational professionals into the design and development of their ISE enhancements.

Section 7 carries forward the discussion of an agile, iterative, human centered design and development methodology begun in Section 6, and then demonstrates it through ongoing collaborative design and development activity with the chief developer of IMDE/CSS, SRI International. This collaboration between MOISA 2 and SRI took the planning and scheduling use case knowledge described in Section 6 and used it to develop a test scenario that drove a series of design-build-evaluate iterations. These "tests" integrate regional operational professionals with system designers and developers in the iterative design of an IMDE/CSS module for a planned regional operational demonstration in 2016. The goal is to demonstrate enhanced regional mission accomplishment of security, safety and resilience operations through use of a planning and scheduling module that lives on a regional enterprise architecture. A key differentiator here is that users are not being asked to test existing or even prototype systems; they are actually joining the team early enough to play a major role in designing their own

solutions, facilitated by professional designers and developers. Thus, Section 7 provides a concrete example of the benefits and challenges of true co-creation with the diverse set of maritime stakeholders. In addition, this approach addresses issues of transition and adoption so early in the process that by the time all stakeholders are satisfied, the system is already "owned" by the community.

MOISA's success has been leveraged by the University of Washington to establish a Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR). Section 8 presents MOISA 2 exploration of a series of potential repeatable mechanisms that would benefit the regional security, safety and resilience community and could be maintained under the CoSSaR umbrella. These include identification of space and initial planning for a regional co-development laboratory, a much needed guide for the handling of controlled unclassified information by non-federal organizations; exploration of a shared survey and regional data archive mechanism, and support for the use of standards in regional information sharing systems. However, the most important repeatable collaborative mechanism developed during MOISA 2 was CoSSaR itself, whose mission is to be "a multi-disciplinary facility and environment where professionals from a wide range of entities (federal, state, county, city, tribal, international, public and private) team with university experts to align strategies, processes and investments in systems for security, safety and resilience."

As described in this report, MOISA 2 has moved forward on a number of fronts to clarify and demonstrate how regional maritime operations can be enhanced through ISE innovations, so long as those innovations are derived from and developed in concert with the diverse regional community of operational professionals who must, in the end, buy into and benefit from them.

2 Introduction

> *[We will] enhance unity of effort through operational planning, logistical support, and execution with DHS, DoD, and other partners… [Excellence] requires the Coast Guard as a whole to foster innovation and partnerships across the public and private sectors.*
>
> Commandant's Direction 2014

The second year of the Maritime Operational Information Sharing Analysis project (MOISA 2) was conducted from October 2014 through September 2015. MOISA 2 built on the understanding and analysis of the Puget Sound information sharing environment (ISE) and the operational practices of Federal, state, local, tribal, international, public and private regional partners (the FSLTIPP) gained during MOISA's first year (see Background). MOISA 2 expanded on the MOISA 1 analysis by focusing on two new use cases – (1) operational planning and scheduling and (2) small vessel security (MOISA 1 had conducted an in-depth analysis of a terminal security use case). In addition to adding new use cases, MOISA 2 extended its MOISA 1 Federal partnerships, consisting of: the DHS Interagency Operations Centers program (IOC); the National Maritime Intelligence-Integration Office (NMIO); and the Program Manager for the Information Sharing Environment (PM-ISE), to include the DHS S&T IMDE/CSS program and its prime developer, SRI International. Thanks to these new partnerships and opportunities, MOISA 2 broke new conceptual and methodological ground in achieving improved information sharing to enhance unity of effort and foster innovative partnerships across the diverse community of Puget Sound maritime security and safety stakeholders.

The USCG Commandant is not the only national leader to recognize that information sharing and partnerships in support of integrated operations are critical to enhancing the security and safety of our country. The 2016 Senate Appropriations Bill (Report 114-68) states that DHS "started as 22 separate agencies and entities and many of those stovepipes remain today, albeit within one department. The Committee supports the Secretary's efforts to break down those silos and, where it makes sense, to push for integrated operations and functions." And in the case of achieving ISE enhancements through new technologies and methodologies –

a central MOISA focus – the Bill states that "the Department must fight complacency and the bureaucratic tendencies that slow its ability to… incorporate new capabilities."

It has been more than a decade since the President directed "the coordination of United States Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, state, local, and private sector entities."[1] Systems intended to enhance inter-agency maritime domain awareness have been envisioned, piloted, and fielded since shortly after this directive, and these initiatives have added to our capabilities in this area. Yet "[t]he question is whether these actions have made our shores more secure from potential maritime threats….The Government Accountability Office, the Department of Homeland Security Inspector General, and the RAND corporation have all raised legitimate concerns…"[2]

Why is it so difficult to achieve the goal of integrated operations supported by shared information? Is it really, as the Senate Bill states, primarily complacency and bureaucracy? Is it perhaps, as Congressman Rick Larson states, an issue of funding? "We cannot expect the Coast Guard to do more with less. The sad reality is that the Coast Guard is doing less with less, and MDA [Maritime Domain Awareness] is no exception."[3] Certainly organizational structures, policies and incentives often make it more difficult to share information and partner on joint operations, and certainly a lack of funding has hampered progress towards systems that enable necessary enhancements to the ISE. MOISA, however, has articulated additional critical barriers to the alignment of FSLTIPP investments, information, and operations that no amount of funding or organizational restructuring can overcome. More importantly, MOISA 2 has taken us from the articulation of these barriers in MOISA 1, to the demonstration of strategies and methodologies that can enable us to achieve our goal.

MOISA tells us that the past decade of investments to enhance information sharing has not had the intended impact because of issues such as:

---

[1] National Security Presidential Directive-41/Homeland Security Presidential Directive-13A, December 21, 2004.

[2] Congressman Rick Larson, Hearing (112-92) before the Subcommittee on Coast Guard and Maritime Transportation, July 10, 2012.

[3] Ibid.

- They put technology at the center of intended enhancements
- They assumed that if Federal agencies took the lead, other non-federal partners would follow
- They employed top-down design strategies
- They underestimated the role of non-federal organizations and assets in regional security and safety
- They failed to recognize the investment as an intervention in an extremely complex and already working regional security and safety service system
- They focused on federally-defined "problems," rather than recognizing that many of these actually represent conflicting stakeholder needs and perspectives
- They failed to include adoption and transition issues from the outset
- They viewed the initiative as ending when it was fielded (or even worse, when the scientific and technical concept was demonstrated)
- They underestimated the role of informal community relationships and interactions
- They underestimated the importance of daily operations

In too many cases, past initiatives have failed to put the people and the community these people work so hard to build and sustain – the work they do and the information they use to do that work – at the center of our efforts to support increased information sharing and collaboration. In short, past work has predominantly been technology centered rather than *human centered.*

Human-centered approaches are dramatically changing how the technology sector designs, develops, introduces, and supports technology innovation, especially where the goal is to positively impact a complex socio-technical system like that which provides security and safety services to our country. (See Section 7.2 for a more in-depth discussion of these changes not only in industry, but in government as well.) Thanks to the support of the Puget Sound security and safety community, our sponsors, and our new partners at DHS S&T and SRI International, MOISA 2 initiated a unique state-of-the-art human-centered demonstration of how to design, develop and transition technology innovation to enhance a regional information sharing environment. While the methodology for such an effort is relatively clear (and described here in Section 7), the accomplishment is not always easy, requiring important levels

of trust and shared understanding across at least four key stakeholder groups: the sponsors, the designers, the developers and the operational community. Achieving this trust and shared understanding takes time and attention (and was a focus of our foundational MOISA 1 effort), but without this trust a human centered effort involving such a complex set of interdependent stakeholders cannot be accomplished. As the saying goes, if you don't have the time and resources to do it right the first time, you certainly don't have the time and resources to do it over and over again. Fortunately, the growing field of human centered design and engineering is training bright young minds and producing creative methodologies to make this process more efficient, effective and evidence based.

The final report of MOISA 1 ended with a promise.

> Rather than dwell on the less than optimal impact of past IT investments, MOISA 1 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.

As reported here, MOISA 2 takes a significant step towards demonstrating the fulfillment of this promise.

3 Background

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. Puget Sound offers a unique 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 (FSLTIPP) entities.

In August 2014 the University of Washington established the Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR), and in September 2014 CoSSaR researchers completed a year-long study (begun before CoSSaR's creation), the Maritime Operations Information Sharing Analysis 1 (MOISA 1). Their findings provide the background and context for this report.

During MOISA's first year investigation, it was found that Puget Sound security and safety stakeholders work on a daily basis to promote and maintain a mature, diverse and dynamic community, and to align their information sharing environment (ISE) with the work that is done both individually and collaboratively in support of their missions. Members of this community view the quality of their trust-based, largely self-organized ISE as a key element of regional resilience, enabling them to complete daily work and to operate in the face of threats to security, safety and resilience. For this community, even during incident response, the National Incident Management System (NIMS) framework does not replace the importance of their extremely rich and nuanced, relationship-based fabric of identity and trust. NIMS is the going in position, but as an incident evolves, the community relies heavily on its already developed fabric of trust to coordinate and innovate. 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 one of their greatest assets.

The ISE of daily operations is not always the same as the ISE of incident response. While non-Federal members of the regional community manage assets that are critical for security, they do not on a daily basis see security as their primary job. 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 ISEs of daily operations and incident response in the Puget Sound security, safety, and resilience community are intimately intertwined because the collaborative work that is done during daily operations facilitates and is foundational to the ISE of incident response.

While Puget Sound security and safety stakeholders work daily to strengthen their relationship-based operational ISE, there are still some critical gaps. Gaps originate from personnel turnover, retirement, lack of understanding or knowledge of partner assets or capabilities, from stove-piped thinking and investment, and from conflicting priorities of missions and cultures. As MOISA discovered in year one, 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 they should receive it; these translate into less effective and responsive action by the community. For this reason, the operational community invests significant time and energy in an ongoing effort to establish trusted relationships and achieve a community that partners towards common goals.

In addition to the informal trust-based relationships, there are numerous formal systems in the Puget Sound region intended to receive, store, and deliver information, generally focused on incident response. 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 identity 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 which shows little interest in or awareness of data standards or meta-tagging or national exchange models.

MOISA 1 confirmed that in order for investments in IT systems to meaningfully impact regional and national security, safety and resilience, these systems must be designed and implemented through methods that center on humans and their missions. MOISA 1 also

introduced a human-centered, model-based methodology for achieving a holistic set of requirements for security system design. This included partnering with community stakeholders to investigate and develop an as-is model of the work processes and information sharing for a container terminal's security-related cargo operations. This model applied and extended the Object Management Group's (OMG) Business Process Model and Notation (BPMN) standard[4] for process modeling, and revealed how partner information sharing is integrally integrated with the accomplishment of the work, as well as the relationships among people, systems and information. This terminal security model provided examples of how this methodology could be used to support system innovation.

During MOISA 1, we found that, to date, federally-centric formal systems, generally delivered as a series of technology-based solutions, have not sufficiently supported the daily work and mission of the community, nor have they been designed to support the strengthening of community trust and self-knowledge. In the past many systems, often funded under short-term grants, have been brought in piecemeal with few plans for sustainability. These initiatives have added new work; generally making current work harder, not easier. Frequently, new systems have not replaced older systems but rather added another layer of technology and work. They typically have not been owned by the community as a whole, and have not been designed based on a thorough knowledge of how the regional community works, how they share information, and how they self-organize. In many instances 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).

As a member of the Puget Sound Area Maritime Security Committee, CoSSaR worked under MOISA 1 to better understand and support the environment for and design of information sharing technologies and strategies for the region. As the second year of MOISA began, CoSSaR was well positioned to take the next steps that are reported in this MOISA 2 completion report.

[4] http://www.bpmn.org

4 Sensors and Sensor Opportunities

The MOISA 2 investigation into regional sensors was initiated by a question at a Puget Sound Area Maritime Security Committee (AMSC) meeting as to whether a survey of sensors in the Puget Sound region was available. As a compilation of sensors did not already exist, a sensor survey task was written into the second year of MOISA to provide the maritime community the information it requested.[5] MOISA conducted a community sensor analysis and – to put the sensors and their usage in context – facilitated a community analysis by sensor owners and potential users of available sensors to determine sensor use and value in mitigating potential threats to or in the maritime environment. This section of the MOISA 2 report presents the results of the sensor survey and the community analysis.

4.1 Puget Sound Sensor Survey

4.1.1 Survey Purpose

In addition to community interest in the sensors operating in the Puget Sound region, the draft National Maritime Domain Awareness Architecture Plan describes a national maritime information sharing environment (MISE) that allows information sharing through common data standards without prescribing how individual agencies perform their mission. A high priority mission that the MISE will support is the detection, classification, and interdiction of small maritime targets. These tasks can be aided by a common maritime domain awareness picture in which data from multiple sensors are integrated and available to the appropriate agencies. The DHS Science & Technology's Integrated Maritime Domain Enterprise/Coastal Surveillance System (IMDE/CSS) project seeks to provide this capability through an enterprise architecture. Therefore, this sensor survey may also contribute to the planned demonstration of IMDE/CSS in the Puget Sound by identifying sensors in use by the maritime community and their physical configuration and specifications.

[5] Cameras were not a focus of this survey, but participants were asked about cameras in addition to AIS and RADAR shore-based stations. While the results presented here contain cameras, this survey does not report all Puget Sound cameras.

This survey does not address data messages, the subsequent use of data, or policies regarding the sensors and data, although subsequent work will address these areas. Previous MOISA research indicates that successful data integration must occur within the context of collaborative regional mission accomplishment.

4.1.2 Survey Geographical Scope

The survey investigated sensors located in the United States Coast Guard (USCG) Sector Puget Sound area of responsibility, including the Puget Sound, San Juan Islands, Strait of Juan de Fuca, and offshore US and Canadian waters. The international border between the US 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 US and Canada to ensure the safety of vessel traffic. The Cooperative Vessel Traffic Service (CVTS), established in 1979, governs the waterway management of the Strait of Juan de Fuca and its connecting waterways. (See *Figure 1*.)

Figure 1: The USCG Puget Sound Area of Responsibility & geographical scope of survey.

4.1.3 Survey Sensor Type Scope

The sensors that are included in the survey are shore-based automatic identification system (AIS) stations and shore-based RADAR stations. As a secondary interest, the survey also investigated stationary cameras.

4.1.3.1 AIS

Automatic identification system (AIS) is a broadcast communications system operating in the VHF maritime band and was first mandated in 2002 to aid in safety of life at sea. Regulation 19 of Safety of Life at Sea (SOLAS) Chapter V – Carriage Requirements for Shipborne Navigational Systems and Equipment requires AIS to be fitted aboard all "ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size." The USCG has amended its AIS requirement to include commercial vessels at least 65ft, towing vessels at least 26ft, 600 horsepower dredging vessels, and vessels carrying certain dangerous cargo (CDC). AIS transmits identifying information such as a vessel's maritime mobile service identity (MMSI) number as well as dynamic data including navigational status, position, course, and speed. AIS consists of on-board equipment and shore-side equipment. An AIS shore station is the physical location that receives AIS messages from transmitting vessels.

4.1.3.2 RADAR

Shore-based marine RADAR has been used for VTS systems since 1948 and is the core tracking technology used in VTS. RADAR provides distance and bearing of detected vessels from the sensor but cannot identify a vessel. RADAR can detect vessels that are not transmitting via AIS; therefore, it is vital in non-cooperative tracking. RADAR is not dependent on other systems, whereas AIS requires GPS. The effectiveness of RADAR can be diminished by weather conditions, gaps in coverage, and overshadowing of vessels.

4.1.4 Survey Data Fields

The survey sought to identify the current configuration of maritime sensors but not capabilities (other than zone of coverage), vulnerabilities, or operational restrictions (other than interference/blockage). Therefore, the data collected is limited to essential sensor identification information, namely:

1. Sensor type and model
2. Owner/operator: who is responsible for keeping the hardware operational
3. Location: GPS coordinates and altitude or approximate location
4. Zone of coverage: including known interference/blockages due to structures

This survey seeks to describe the numbers of sensors in the area, their physical configuration, and the overall coverage.

4.1.5 Survey Response

The tabular and graphic representation of the sensors compiled by MOISA in the sensor survey are controlled as "For Official Use Only" (FOUO) and can be obtained by contacting the Center for Collaborative Systems for Security, Safety, and Regional Resilience (CoSSaR) at the University of Washington. Sensor information was provided by the Marine Exchange of Puget Sound, the USCG Sector Puget Sound Joint Harbor Operations Center (JHOC), the Royal Canadian Mounted Police, Port of Bellingham, Port of Olympia, and the Customs and Border Protection Office of Air and Marine. Washington State Ferries declined to participate due to security concerns. There was no response from the United States Navy, USCG VTS, Port of Tacoma, Port of Seattle, Port Metro Vancouver, Port of Everett, Port of Port Angeles, Shilshole Bay Marina, Squalicum Marina, Port Townsend Marina, and the United States Army Corps of Engineers.

The sensor information for the USCG was obtained from the Department of Homeland Security Interagency Operations Center Sensor Survey Report for USCG Sector Command Center Seattle (November 2010). We appreciate USCG providing access to this FOUO document.

For those agencies that did respond, only the Marine Exchange of Puget Sound (MXPS) and USCG provided exact locations. The other respondents did not wish to provide the requested level of detail regarding location due to security concerns. Zone of coverage and known obstructions was also a data field that was answered at a high level if at all.

4.1.6 Maritime Security Operations Centre

The Marine Security Operations Centre (MSOC) in Victoria, British Columbia is a collaborative effort among the Canadian Border Services Agency, Canadian Coast Guard, Department of National Defence/Canadian Forces, Royal Canadian Mounted Police, and Transport Canada. While the primary mission of the CVTS is the safe operations of commercial traffic, the mission of MSOC "is to provide Canadians with comprehensive marine security to detect, assess, and support appropriate response to marine based threats that could negatively affect the safety, security, environment or economy of Canada (Marine Security Operations Centres Project. (2013). http://www.msoc-cosm.gc.ca/en/about-us.page Accessed 31 January 2014)."

The Canadian Coast Guard has complete AIS coverage of the northern Puget Sound area (coverage in all Canadian waters and good coverage of line of sight into US waters). The RCMP has access to this data for law enforcement and security needs. The RCMP and Canadian Coast Guard operate a radar system capable of small vessel detection and tracking. There is significant coverage from Vancouver Harbour to the Pacific coastline west of Cape Flattery (WA) and Vancouver Island (BC). This tracking means that any vessel regardless of its participation in the traffic system is detected and tracked automatically. This can be monitored and relayed to enforcement units in real time and can be monitored at several RCMP locations including mobile units.

4.1.7 Summary of Sensor Survey

The Puget Sound regional sensor survey provides information from multiple agencies at the level of detail that agencies were willing to share, and provides the first iteration of what could become a valuable, if sensitive, community resource that should be expanded to include

additional sensor locations and types (e.g. mobile sensors). Copies of the complete survey can be requested through the Center for Collaborative Systems for Security, Safety, and Regional Resilience (CoSSaR) at the University of Washington.

This sensor survey also provided input to a series of workshops, reported on below, that analyzed the potential value of integrated sensor and other data for use in mitigating potential threats in the maritime environment, particularly within the context of a planned DHS regional enterprise architecture.

4.2 Community Sensor Workshop Analysis

4.2.1 Workshop Information

As a follow-on activity to the regional sensor survey conducted by MOISA in early 2015[6], the research team conducted a series of workshop sessions around the Puget Sound region to learn more about perceptions and uses of sensors in the region. Our initial sensor survey was limited to fixed sensors (i.e., shore-based AIS, RADAR, and camera sensors) in the United States Coast Guard (USCG) Sector Puget Sound area of responsibility[7] and the sensors' physical configuration. An additional focus in the workshops was to identify other data sharing opportunities as well as possible opportunities for mission enhancement through the integration of data via the IMDE/CSS demonstration.

In the workshop sessions, we invited the larger regional maritime community to come together to discuss additional maritime sensors in our region, the use of data from regional sensors for mission accomplishment, the potential advantages and disadvantages of sharing sensor data, and constraints on such sharing. The workshop discussions covered both fixed and mobile sensing of vessels of all sizes operating commercially, recreationally, or for homeland security, defense, and law enforcement purposes.

[6] Puget Sound Sensor Survey: Shore-based AIS, Radar, and Camera Sensors, MOISA, March 2015. This survey is a FOUO document that can be requested by emailing moisa@uw.edu.
[7] The AOR includes the Puget Sound, San Juan Islands, Strait of Juan de Fuca, and offshore U.S. and Canadian waters.

In this section, we present the key ideas that emerged from these workshop sessions. We also include details about how we conducted the sessions and unique discoveries from each session. We conducted the workshop sessions at four different regional locations to encourage participation (through travel convenience) and to capture geographical differences in mission and work environments.

4.2.1.1 Workshop Session Methodology

Each workshop session lasted approximately 90 minutes during which the participants engaged in an open discussion of topics introduced by the facilitator. In each session, notes were taken on a flip-pad at the front of the room and additional notes were taken by at least two members of the research team.

General Topic 1. Findings of the Sensor Survey followed by a discussion of how sensor data currently contributes to organizational missions and could further contribute in the future.

- Are there other sensors not included in the sensor survey results?
- Is there anything that you do that suffers from lack of data?
- Can you identify opportunities for improved mission accomplishment through increased sensor data access/sharing?
- If access to regional sensor data was expanded, would you use the data on a daily basis versus in the event of an incident?
- Assuming you had access to this additional sensor data, what else would you need to benefit from this access?

General Topic 2. Discussion of constraints to sharing and using sensor data.

- What currently prohibits you from sharing your sensor data or receiving data from others?
- If you decided to share your sensor data, what changes would you need to make to your current operation, such as additional human or technical resources, policy adjustments, mission modifications, risk analysis, etc.?
- If you received sensor data from others, are there barriers to using it?

While the workshops were held to discuss sensors and sensor data, the participants offered additional insights into information sharing. Opportunities and barriers that apply to information sharing in general will apply to sensor information sharing as well. It is also worth noting that IMDE/CSS was not the focus of the workshop discussions. It was briefly mentioned as a motivating factor for conducting the workshops, but the comments summarized in this report are not in response to the community's evolving perception of the IMDE/CSS project. This analysis serves a larger purpose of discovering information sharing needs and perceived barriers. This understanding of the community can then be used when evaluating any technology intended to improve the information sharing environment, including IMDE/CSS.

4.2.1.2 Workshop Sessions

1. **Seattle, WA**

   Date: 13 April 2015

   Location: University of Washington, Sieg Hall Room 420, Seattle

   Time: 1400-1600

   Agencies Represented:

   - Drug Enforcement Agency (DEA)
   - Homeland Security Division for Washington State Patrol (WSP)
   - King County Sheriff's Office Aviation Support Unit (KCSO AUS)
   - Marine Exchange of Puget Sound (MXPS)
   - USCG Station Seattle
   - Washington State Fusion Center (WSFC)

2. **Tacoma, WA**

   Date: 14 April 2015

   Location: Silver Cloud Inn, Boardroom, 2317 Ruston Way, Tacoma

   Time: 1300-1500

   Agencies Represented:

   - APM Terminals
   - Drug Enforcement Agency (DEA)

- Northwest Regional Aviation
- Pierce County Sheriff's Office
- Port of Tacoma
- Pierce County Emergency Management
- Western Air Defense Sector (WADS)

3. **Port Townsend, WA**

   Date: 21 April 2015

   Location: Northwest Maritime Center, 431 Water St, Port Townsend

   Time: 1100-1300

   Agencies Represented[8]:

   - East Jefferson Fire Rescue (EJFR)
   - Jefferson County Sheriff
   - Northwest Maritime Center (NWMC)
   - Air Station/Sector Field Office (SFO) Port Angeles

4. **Blaine, WA**

   Date: 22 April 2015

   Location: Blaine Border Patrol Sector, Headquarters Conference

   Room, 2410 Nature's Path Way, Blaine

   Time: 1000-1200

   Agencies Represented:

   - CBP - Intel
   - CBP - OAM
   - Coupeville Police Chief
   - Royal Canadian Mounted Police (RCMP)
   - Port of Everett
   - Washington Department of Fish and Wildlife (DFW).

[8] A member of the MOISA sponsor team representing the National Maritime Intelligence-Integration Office (NMIO) was present at the Port Townsend and Blaine workshops.

4.2.2 Sensors the Community Uses

Each workshop began with an overview of the 2015 Sensor Survey and a prompt for other sensors that the participants use or know of that are not included in the survey. Significant additions included the Churchill Navigation® Augment Reality System (ARS), downlink capabilities, onboard mobile RADAR, people, and in the future, drones. See Table **2** for a complete listing.

The ARS combines parcel data, address information, street maps, video, infrared video, and AIS data into one display in an aircraft. The capabilities of the ARS allow the pilot to mark an oil sheen and track its growth, as well as letting the pilot drop a virtual marker at a location and directing the pilot back to that location at a later time.[9]

Downlink capability refers to the ability to allow remote viewing of assessments via real-time microwave video downlink; in the case of King County Sheriff's Office Aviation Support Unit (KCSO ASU) remote viewing takes place in the King County Regional Communications and Emergency Coordination Center, the mobile command post, and other locations, such as the Sensor Management System in the Joint Harbor Operations Center (JHOC) and Carry Viewers within line of sight.[10] A representative from a USCG Small Boat Unit reported that a significant proportion of public requests to investigate a "small boat"[11] were either false reports or resulted in no need for action. Sending an aircraft with downlink capability to investigate ahead of the small boat unit could reduce wasted USCG efforts.[12] Several participants reported that the network support for video downlink is old and outdated; this limits the usefulness of the downlink capability.[13]

Workshop participants obtain a significant amount of information directly from employees and people at the scene, e.g., a 9-1-1 caller. Generally, the first people to the scene

---

[9] King County Sheriff's Office Aviation Support Unit. 13 April 2015. Seattle Sensor Workshop.
[10] King County. (2014). King County, Washington Emergency Management Plan, Emergency Support Function 13 Public Safety and Security.
[11] Several reports of small boats are other objects such as buoys and logs.
[12] USCG Small Boat Unit. 13 April 2015. Seattle Sensor Workshop.
[13] "WSP microwave towers can't take on more services. An upgrade is needed to use video downlink capability on a regular basis." - KCSO ASU

are not federal. Most patrol vehicles and vessels have GPS and AIS, respectively, to allow location tracking.

The future use of drones came up in all workshop sessions. Community members are excited about the possibility of drones providing useful data, however, they are concerned that the regulations for drone use (especially recreational) need to be refined to avoid conflicts. The USCG gave an example of a recreational drone that was too close to an incident for the USCG helicopter to approach.[14]

Table 2: *Sensors/Equipment Used by the Community*

Agency	Equipment
Air Station/SFO Port Angeles	- FAA Radar - No downlink, no AIS - 3 helicopters with FLIR
APM Terminals	- WSDOT land-based water-facing cameras
East Jefferson Fire Rescue	- Civilian weather stations - Person with last visual contact with vessel (over phone) - Two vessels (33' and 21') with RADAR, FLIR
Coupeville Marshal's Office	- FLIR and radar on boats
Jefferson County Sheriff's Office	- Marine patrol vessel
KCSO ASU	- 3 helicopters - FLIR, 2 mile range, real-time - Night vision goggles - Churchill Navigation® Augment Reality System - Video downlink from aircraft
Marine Exchange of Puget Sound	- Included in 2015 Sensor Survey
Northwest Regional Aviation Group	- Low light cameras - Downlink stations to get imagery from Bellingham to Olympia
Pierce County Sheriff's Office	- 36' SAFE boat with AIS, Furuno Radar, FLIR, no rad/nuke - 2 aircraft; 1 with FLIR, ARS, video recorder, and real-time video downlink capabilities
Pierce County EOC	- Cameras at county ferry terminals
Pierce County Emergency Management	- Steerable, mobile "pole cameras"
Port of Everett	- 57 point, tilt, zoom (PTZ) cameras, JHOC has access to 9, some are infrared - hosts an AIS receiver but no RADAR

[14] USCG Port Angeles. 21 April 2015. Port Townsend Sensor Workshop.

Snohomish County Sheriff's	- 2 aircraft, 1 with FLIR, downlink capabilities
USCG Station Seattle	- Encrypted AIS on small boats - RADAR on small boats
Washington State Patrol	- GPS-equipped vehicles and people - 7 aircraft (2 with FLIR) - ARS - Optical and thermal cameras - Department of Transportation highway cameras
Western Air Defense Sector	- USN subsea buoys - UAVs - Ground vibration sensors

4.2.3 Key Ideas

4.2.3.1 Overall Key Ideas Emerging from Workshop Sessions

A set of high-level perceptions were shared by a broad group of workshop participants. These perceptions were not uniformly discussed by participants in each session, but were reflected in more than one session discussion. The overall take-away is that the community wants information sharing to be mutual, necessary, and tailored. Other shared community perceptions were that:

1. Mobile sensors are of increasing importance but they present inherent difficulties with both data quality and data sharing.[15]
2. Information sharing in an incident-driven scenario is recognized as desirable, but widespread information sharing during routine day-to-day activities is perceived as a burden.[16]
3. More knowledge and transparency about capabilities that exist beyond their immediate organizations is desirable, e.g., a current inventory of community-held regional assets.

[15] Mobile sensors produce less reliable data due to interference from weather and changing obstructions. East Jefferson Fire Rescue has radar and FLIR on-board their vessels, but these sensors do not aid in locating vessels in rough weather since they cannot see over wave crests when in troughs.
[16] There is a widespread perception that more information sharing is desirable, but it was difficult for participants to offer specific examples of incidents that would have benefited from more sharing.

4. Local and state law enforcement appreciated the opportunity to interact with the broader community in these discussions made possible by MOISA; many were willing to coordinate their resources with federal agencies where appropriate.

5. More brokered agreements to enable information sharing would be valuable, particularly in situations where it would be a win-win proposition for all parties involved. See Section 4.2.4.3 for further discussion.

6. Derelict (i.e., unpiloted) vessels and mistaken emergency tips from the public are a burden for the USCG in particular and the community as a whole[17].

7. The ability to collaboratively track a vessel through different areas of responsibility is desired, particularly by federal agencies such as DEA and CBP.

8. Reliance on grants, such as the annual Port Security Grant Program, often results in people buying technologies that are disconnected from one another and not sustainable beyond the award. See Section 4.2.5.5 for further discussion.

4.2.3.2 Session Unique Discussions

In each of the workshop sessions, some ideas brought up in the conversation were unique to that session. In part, these unique ideas reflected different geographical concerns or the composition of the participant group, e.g., roles and organizations represented.

1. **Seattle**
   - Participants focused on "legal" barriers[18] to sharing sensor data and related information.
   - Some participants stated that they do not want more data because they do not have the capability to manage it or analyze it. Additional data also creates expectations that they must do something with it.

[17] Different agencies in the region have their own procedures for addressing reports of derelict vessels. In addition, there is a multi-agency working group in the region that addresses this challenge in the maritime community.

[18] While the participants referenced the legal barrier created by the Public Records Act and the FOIA as reasons they do not record data, they were referring to their policies of not recording or storing data to reduce the amount of information that is available to be requested under the law.

- Some sensor capabilities mentioned were not previously known by the other participants.[19] In other words, the workshops served as a mechanism for community sharing of capabilities.
- Desire for additional sensors was identified, such as the desire by DEA for radar in Neah Bay where there is a lot of small vessel traffic but inadequate radar coverage.

2. **Tacoma**
   - Issues related to information sharing among military and law enforcement entities were more prominent in this workshop session than the others.
   - Participants desire the ability to turn on/off data and information sources on an as-needed for mission requirements basis.
   - There are legal barriers to sharing between civilian and military sources.
   - The Port of Tacoma perceived too much risk to share its sensor locations with others. However, see Section 4.2.4.3.

3. **Port Townsend**
   - There was a general sense that things are working well.
   - USCG does not have real-time video and data sharing ability from its helicopters, whereas King County helicopters do.
   - For state-funded agencies, there is a strong focus on boating safety rather than other forms of law enforcement in their maritime operations.
   - There is an assumption that VTS data is already shared across entities in the community. The workshop USCG participant reported that VTS information cannot be used for anything other than VTS services.[20]

---

[19] For example, participants were unaware of the KCSO ASU downlink capability and the Air Force Rescue Coordination Center's cell phone triangulation capability. See discussion in Section 4.2.5.3.

[20] Outside the workshop sessions, our team was informed by NMIO that "raw radar data from the Cape Flattery VTS sensor is passed to Canada Coast Guard, who passes it on to Canadian RCMP for specialized processing to detect and track small vessels. That data is then used by Canada for law enforcement purposes. The US Coast Guard VTS Program Office has authorized that data sharing and is fully cognizant of its use by the Canadians. At this time the results of the specialized Canadian

- There is a perception that 9-1-1 call centers do not know what questions to ask in a water-related incident. In the Port Townsend area, 9-1-1 calls are routinely routed to the wrong call center, sometimes even going to Canada. Rerouting the call results in excessive time delays. 9-1-1 algorithms direct the operator to call USCG. The JHOC serves as the USCG's dispatch and will communicate with the 9-1-1 call center.
- Participants discussed potential methods, e.g., RFID, to mark derelict vessels.[21]
- Federal navigable waters are the USCG's responsibility,[22] though they are also patrolled by US CBP and DEA for specific law enforcement purposes.[23] Local agencies do not have a reason or the resources to be outside of their local area of interest,[24] except in special circumstances when requested.

4. **Blaine**
   - Issues related to the CBP mission (e.g., border control and security) were more prominent in this workshop session than the others.
   - Operational security was a significant concern for federal agencies operating near the Canadian border. CBP indicated they require full control of access to their information.
   - Federal agency employees emphasized that they are required to follow agency-mandated policy when sharing information. Decisions about information sharing are not at the employees' discretion.

---

processing is not being passed back to the US, but US CBP has expressed an interest in receiving this information from Canada and discussions are underway seeking a way to accomplish this feedback."

[21] The Washington State Department of Natural Resources funds and runs the Derelict Vessel Removal Program. For more information see \url{http://www.dnr.wa.gov/Publications/aqr_dv_guidelines_0907.pdf

[22] 33 CFR 329.4: Navigable waters of the United States are those waters that are subject to the ebb and flow of the tide and/or are presently used, or have been used in the past, or may be susceptible for use to transport interstate or foreign commerce. A determination of navigability, once made, applies laterally over the entire surface of the waterbody, and is not extinguished by later actions or events which impede or destroy navigable capacity.

[23] According to the Clallam County Sherriff, CBP sometimes has personnel accompany their office on patrol boats. These arrangements are discussed further in the <<small suspicious vessel>> section of the MOISA II report.

[24] Some areas of jurisdiction overlap with others geospatially.

- There were, however, examples of enhanced information sharing based on past relationships and experiences, e.g. between members of CBP and DFW.
- Spillman technologies (see Section 5) are used by some law enforcement entities at the port and county level, but budgets limit how extensively they are used.
- Among non-Federal agencies, participants expressed a desire to share information on an as-needed basis. These members of the community see a difference between information availability and information sharing. They prefer knowing what sensors exist and that their information feeds are available if requested, rather than constant sharing and monitoring of a 24/7 information feed.

4.2.4 Desired Information Sharing Environment

4.2.4.1 List of Resources and Capabilities

Many workshop participants desired a shared secure list of agency resources and capabilities. They indicated, however, that they generally do not have the need for and resources to handle and process all the information that would be available in an all day, every day situational awareness system. For instance, the Washington Department of Fish and Wildlife (DFW) stated:

> "If there are things people are specifically looking for, we can look for it, but going out every day to record everything raises personnel-power and cataloging issues."

Overall, the participants seemed wary of generic 24/7 information sharing and would rather increase awareness of who has what so that the specific asset/information can be requested on a case-by-case basis. However, the volume and type of information desired by different agencies with different missions is not uniform. While most agencies expressed a desire for information on an as-needed basis, some wanted certain types of information pushed to them in a continuous feed (e.g. CBP wanted all border crossings).

The workshops reinforced the conclusion from MOISA 1 that a significant amount of information sharing in the community is based on personal relationships. DFW questioned how the knowledge of who has what can be passed on to incoming personnel without those

relationships. DFW suggested a master list that is regularly updated. A port security grant was given to the Marine Exchange of Puget Sound to develop an inventory of equipment procured and systems developed under PSGP funding; this inventory, however, does not include data sources, is marked as Sensitive Security Information (SSI), and has not been widely distributed. The Port of Everett wants lists like these to be electronically accessible and secure.

A key piece of information to be included in a master list is the response time of agency assets to various places within the area of responsibility (AOR). According to the CBP-OAM, the Puget Sound AOR is a small sea space with hard boundaries that limit the time available for response/interdiction. Knowing ahead of time who can respond in a timely fashion and real-time data on who is actually responding would be extremely useful.

A list of resources and capabilities could satisfy the expressed community need for tailored and necessary information. A well-organized master list could allow people to access only the useful subset of information they needed at a given time. The potential downside of a by-request information sharing model is that the requester might not know what to request, often phrased as "you don't know what you don't know."

4.2.4.2 Dynamic Access Control

The fear of the wrong people gaining access to their information was brought up repeatedly. There was some discussion of various access management approaches. Researchers noted the discussion of these approaches in identity, credential, and access management (ICAM) literature.

For example, the Western Air Defense Sector (WADS) suggested that restrictions on information access to be subject to the type of work, e.g., aviation, maritime, military, search and rescue. (This approach is called **role-based access control**.[25] During maritime incidents and day-to-day operations, there is "rapid change in membership of coalitions and the roles of

[25] The roles can be, for example, intelligence officer, law enforcement officer, military officer, etc. McDaniel, C.R. & Tardy, M.L. (2005). Role-based Access Control for Coalition Partners in Maritime Domain Awareness, NPS Thesis. www.dtic.mil/dtic/tr/fulltext/u2/a435572.pdf

coalition participants."[26] By controlling access based on roles rather than individuals, this approach attempts to assure that the appropriate people can quickly access the information relevant to their missions.)

Northwest Regional Aviation had a different perspective. They share imagery informally but want the ability to restrict access based on information sensitivity, including the ability to modify that access based on the nature of the mission being executed. (This approach is called **temporal access control**. From this approach, access to the resources/ information can be requested and temporarily enabled and then disabled when an operation is complete. Dynamic access control, however, requires that community members know who has what and who needs to know what information. It is unclear if individual agencies should be responsible for maintaining this awareness or if a central organization (i.e., operations center) should act as an "information broker".[27])

4.2.4.3 Reciprocity and Transparency

While many workshop participants expressed concerns that made them reluctant to share information, it was clear that they were willing to participate in an information sharing environment if they received something in return, whether that was information they needed or other reciprocities. For example, the Port of Everett stated that they were willing to share their camera feeds with their Navy neighbors, if in return they could see the feed from the Navy's next door cameras. This situation is particularly interesting because each set of cameras can see under their neighbor's dock, but not under their own.

In a somewhat different example, the Port of Tacoma, who had chosen not to share even the location of their cameras, expressed concern about their ability to look out over the water at night. When asked if they would share their camera feeds with Federal partners if given infrared cameras, they said yes, provided they knew with whom they were sharing. This potential "barter system" has important implications for improving the regional information sharing environment.

---

[26] Ibid.
[27] Ibid.

Agencies that expressed an interest in having more information shared with them (e.g., CBP) said that they could not share some of the information they possess because of the potential risk to their ongoing mission. Limitations like this can make it difficult to establish a fully reciprocal information sharing system.

4.2.5 Other Barriers to Sharing

4.2.5.1 Washington State Public Records Act

The Washington State Public Records Act (PRA),[28] RCW 42.56, was passed by Washington voters in an earlier form in 1972 with the main goal of campaign finance and lobbying reform; the law was recodified in 2006. The PRA allows anyone to request any state or local public record[29] with no requirement to express their intended use of the data.[30] There is a set of exemptions to the PRA that is regularly reviewed by the public records exemptions accountability committee. Chapter 40.14 RCW Preservation and Destruction of Public Records contains the policies governing how long public records must be retained.

In every workshop session, the Washington State Public Records Act (PRA) was mentioned as one of the main reasons the participating agencies do not record or receive data. An example of the burden a PRA request can place on an agency is illustrated in a Seattle Times article from 2014 in which

> "The city's chief technology officer, Michael Mattmiller, told The Times on Wednesday that the city receives about 6,000 public-disclosure requests each year, a number that he said has been increasing. Recently, Mattmiller said, the city received a request for all emails received and sent by city employees. If fulfilled, the request could cost the city

[28] The Act's purpose is stated as: "The people of this state do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created."
[29] The statute defines "public records" as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency."
[30] There is no state equivalent to FOUO or SSI that prevents public release.

> $110 million in salary and take 1,376 years for one full-time employee to respond, he said."[31]

For this reason, the King County Sheriff's Office (KCSO) Aviation Support Unit (ASU) and Pierce County Emergency Management do not record data. KCSO ASU will pass helicopter video to another agency that can record the data if it wishes to, but KCSO ASU itself does not record any video. Washington State Patrol obtains video data in a way that is harder for them but is also harder to request through the PRA. Washington State Patrol remarked that

> "Some people won't push data because it will be released. There is some information we don't want because we don't want the hassle of public disclosure."

Video is particularly sensitive as it has become vital to prosecution. DEA reported that "video has become all important; the jury wants to see video."

Balancing the right of citizens to oversee and engage with Washington State public agencies with the burden of fulfilling PRA requests is an ongoing challenge for all state agencies. What are perceived by agencies as unreasonable citizen requests and the resulting incentive to reduce their catalog of public records has led to calls for a change in the PRA.[32]

4.2.5.2 Technological and Operational Security

Workshop participants pointed out that it will only take one security breach for everyone to want to pull their information out of the system. The Port of Everett stated that "Once people are caught looking at stuff they are not supposed to or misusing information, everyone will pull back their assets from the system." For RCMP to engage in a system, their IT department would need to sign off on its integrity. RCMP stated "For anyone in law enforcement there has to be confidence in [the system] before there will be sharing." RCMP also reported that US VTS is hesitant to let others use their data: "The biggest barrier is convincing the VTS people that we are not going to break their systems."

---

[31] Sullivan, J. (20 November 2014). Man drops massive records requests, will help Seattle police with video technology. Retrieved April 29, 2015, from http://www.seattletimes.com/seattle-news/man-drops-massive-records-requests-will-help-seattle-police-with-video-technology/

[32] School District struggles under weight of the Open Public Records Act. (7 January, 2015). Retrieved June 7, 2015, from http://www.southwhidbeyrecord.com/news/287705711.html

The integrity of access control to the system was also a concern. Canadian RCMP stated, "We are working with information that if released, people will die." CBP reported "I don't want anyone to know where my boats and operations are or what my staffing levels are...that is the problem with HSIN. I don't know who else is looking at [my information]." CBP worried that shared information would be susceptible to Freedom of Information Act requests. RCMP reported that they are allowed to share their VTS information with the USCG, but CBP reported that the Canadian Coast Guard is not cleared to know US operational security information. Operational security is part of the reason the US Navy does not transmit AIS or follow the "rules of the road,"[33] both of which present safety concerns to the workshop participants.

4.2.5.3 Law Enforcement Legal Restrictions

Workshop participants indicated that legal restrictions on law enforcement agencies affect how they engage in information sharing actions. For example, the King County Sheriff's Office Aviation Support Unit (KCSO ASU) identified a service provided by the US Air Force Rescue Coordination Center (AFRCC) that can triangulate a cell phone in 30 minutes within 100 yards. The DEA said in a life or death situation using this service would be alright; otherwise it would require a large amount of paperwork. Washington State passed a law, HB 1440, in May 2015, that requires a warrant before triangulating a cell phone (the name for this technology is *Stingray*).[34]

We also heard about information sharing barriers stemming from different agencies operating under incompatible policies and laws. For example, under the common law, a police officer is "considered to be under a duty to respond as police officers 24 hours a day."[35] However, KCSO ASU reported that the FBI restricts off-duty officers from running names

[33] The rules of the road is the colloquial term for the International Regulations for Preventing Collisions at Sea 1972 (Colregs) which prescribe what two vessel must do when interacting, *e.g.*, overtaking, passing.
[34] Chris Soghoian, a principal technologist for the ACLU stated that HB 1440 is "the most pro-privacy Stingray law in the country." Washington state limits Stingray surveillance in unanimously approved pro-privacy law. (May 12, 2015). Retrieved May 31, 2015, from http://rt.com/usa/257865-washington-state-stingray-signed/
[35] 16A Eugene McQuillin, The Law of Municipal Corporations Section 45.15, at 123 (3d rev. ed. 1992). See also State v. Wilen, 4 Neb. App. 132, 539 N.W.2d 650, 658 (1995).

through the National Crime Information Center (NCIC) database (even when working under second jobs as security officers when off-duty).[36] KCSO ASU sees this as a barrier; the FBI views the information as confidential and requires that the information be accessed only by an official acting within a criminal justice agency. The FBI has a culture of information safe-guarding and does not easily share information. The Washington State Fusion Center, whose objective is to fuse data from multiple sources, both unclassified and classified, stated that, "the FBI mostly only tells WSFC things that they don't mind being in the *Seattle Times*."

Another issue that was cited often was the lack of information sharing between law enforcement and fire departments. Law enforcement cannot formally share information with the fire department due to restrictions on law enforcement sensitive (LES) information. The fire department cannot formally share medical information with law enforcement. The event to which a fire department is responding may transition into a law enforcement incident, but the fire department's primary concern is still safety of life. East Jefferson Fire Rescue (EJFR) stated "We are not a national security platform; that is not what we are here for." EJFR went on to say that they receive many requests for data they have, but when they ask for data it is generally not provided.

DoD participants in the Tacoma workshop discussed legal barriers to information sharing between military and law enforcement agencies. (For more information, see Appendix A:)

4.2.5.4 Organizational Mandate

Workshop participants also described information sharing barriers associated with different organizational mandates, as in the case of using CG VTS data for suspicious small vessel tracking.

[36] "Employees shall not run names or make inquiries through NCIC III, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer." Seattle Police Department. (2015). 12.050 - Criminal Justice Information Systems. Retrieved May 31, 2015, from http://www.seattle.gov/police-manual/title-12---department-information-systems/12050---criminal-justice-information-systems

The Puget Sound Vessel Traffic Service (VTS) was established by the USCG in 1972 in order to improve the safety of vessels in congested waterways. The purpose of Vessel Traffic Service Puget Sound is

> "to facilitate the safe, secure and efficient transit of vessel traffic to assist in the prevention of collisions or groundings that could cost lives, property damage, or subject the pristine waters of the Salish Sea to environmental harm. The primary function of VTS Puget Sound is to facilitate good order and predictability on the Salish Sea waterways by coordinating vessel movements through the collection, verification, organization, and dissemination of information."[37]

Puget Sound VTS uses AIS and radar to track large commercial vessels. Currently, Puget Sound VTS cannot see small vessels due to the way its radar processing is configured. Canadian VTS can see both small and large vessels using SIGNALIS radar integrator technology. SIGNALIS does the digitization of the signal, the processing, track correlation, and all other system functions. Most of the performance comes from the infrastructure (i.e., height above water, tower height, etc.) and the processing of the signal to detect and track small vessels.

Puget Sound VTS could provide this capability, but given its organizational mandate to increase commercial traffic safety, there was concern among Coast Guard and others that security duties might jeopardize this mandate. A professional mariner at the Port Townsend workshop stated that the value of VTS to him is not national security but rather its role in safeguarding his ship, crew, and passengers. The overwhelming impression from the local workshop participants was that a primarily concerned with safety, and they pointed out that state funding is primarily directed to boating safety issues, not specifically to security.

While the SIGNALIS approach offers the possibility of adding the small vessel tracking capability without impact on commercial safety mandates, it is important to recognize the concerns of the local community that this needs to occur without impact on current Coast Guard operations and the accomplishment of the region's safety mandate.

---

[37] USCG. (2013). VTS Users manual 2013 Edition. http://www.uscg.mil/d13/psvts/docs/userman032503.pdf

4.2.5.5 Funding

The IMDE/CSS project was introduced to help motivate workshop discussion, and this led participants to consider the question of funding to support participation in regional initiatives such as an enterprise architecture[38]. East Jefferson Fire Rescue stated:

> If they have funding either directly or through subsidies, they will participate. If they do not have funding, it is more difficult. Any agency will do everything for SAR [search and rescue], but for other missions like security, organizations will not give you the time of day without funding.

A general concern was expressed that reliance on grants, such as the annual Port Security Grant Program, has resulted in people buying equipment or developing systems that are not regionally coordinated, do not have funding beyond development for maintenance and operations, and are not aligned with a common regional strategy. An example was maritime focused enhancements made to the Spillman system under Port Security Grant funding that were available in one county but not in the neighboring county.

4.2.6 Way Forward

At the end of each workshop, discussion turned to what the participants would like to see in the IMDE/CSS operational demonstration planned for 2016.

The main interest from federal agencies was national security. Federal agencies were interested in demonstrating the capability to follow a small non-AIS transmitting vessel coming from Vancouver Island through the Ballard Locks into Lake Washington. The outcome would be the identification of which agencies can detect, track, and interdict the vessel and when/where they can do so. Another federal interest was tracking a container with illegal contents destined for Puget Sound coming from a foreign port with low security.

[38] Workshop participants were asked to envision a system in which cost was not a consideration. Despite this, some participants addressed cost issues.

The military participants were primarily interested in demonstrating that, whatever the exercise, the information exchange is timely. In past experience, information sharing fails at the seams between agencies. A suggested military-related exercise was the detection and tracking of a small vessel conducting simulated mine laying, which is the focus of an Area Maritime Security Committee (AMSC) exercise scheduled for November 2015.

State and local agencies suggested activities that focused more on specific needs. Law enforcement would like to exercise the downlink capability between Washington State Patrol and King County paying special attention to encryption. The fire department would like to demonstrate the ability to maintain situational awareness through mobile applications. Local agencies, especially those not serving a large city, do not have access to resources such as command vehicles and need accurate and timely information on their mobile devices. More remote local agencies would also like to demonstrate coordination between federal and local agencies in which the local agency is the most proximate asset, i.e., first to respond, to a federally identified incident.

Generally, all workshop participants expressed some interest in strengthening their interagency collaboration, independently and through regional demonstrations.

5 Technology Analysis: IMDE/CSS and Related Regional Systems in Use

5.1 Summary

In MOISA 1 we used a community-centered approach to engage with operational users in the Puget Sound to explore the technology components of their Information Sharing Environment (ISE). We first conducted semi-structured interviews with this population to gather information on the systems used to enable situation awareness. We supplemented these 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. Finally we immersed ourselves into the community by participating in and observing local and regional events, conferences, and presentations. While we discovered that the reliance on information and communication technology was less than one might expect (a replication of MOISA 1 findings), the Puget Sound maritime community does use numerous systems to collect and share data. The three systems that were mentioned most frequently were: (1) the Homeland Security Information Network (HSIN); (2) Spillman; and (3) CommandBridge (a module of what is now called the Washington Common Operating Platform -- WA-COP). In addition to IMDE/CSS, these three systems became the focus of our investigations.

The Integrated Maritime Domain Enterprise/Coastal Surveillance System (IMDE/CSS) project is a Department of Homeland Security Science &Technology (DHS S&T) Borders and Maritime Security initiative. IMDE provides an enterprise architecture intended to support an ISE that will enable operations in an unclassified multi-agency environment. CSS provides a user-defined operational dashboard with new operational functionality and integration of maritime sensors regardless of who owns the sensors. As IMDE/CSS is still in development, we chose to concentrate our efforts not only on a comparison of the three regional systems to IMDE/CSS, but also on how those systems might be used in the future in conjunction with IMDE/CSS.

This section provides an overview of the proposed functionality of IMDE/CSS and three other enterprise systems being used in the Puget Sound; describes how the functionality of these systems map to IMDE/CSS; details how these systems implement data sharing; explains how security is handled; and addresses issues associated with how the data from these three systems could be integrated into the IMDE architecture. We begin by explaining the objectives of this chapter, describing the methodology used to understand IMDE/CSS as well as these three systems of interest, and provide an analysis of the current systems and technologies in use by the Puget Sound maritime community.

5.2 Objectives

The objectives of the MOISA 2 directed tasks addressed here were to:

- Conduct a review of IMDE/CSS architecture, capability, and functionality.
- Conduct a comparison analysis with at least two of the major local systems. The systems chosen were the Homeland Security Information Network (HSIN), Spillman, and the CommandBridge module of WA-COP.
- For each system, identify purpose, user-base, functionality, architecture, opportunities and constraints.

5.3 Methodology

To understand the functionality, architecture and data of the identified systems, we reviewed the available user and technical documentation for all systems. We also conducted telephone interviews with sales, technical, and support staff from HSIN, Spillman and WA-COP/CommandBridge as well as with the developers of IMDE/CSS, SRI International. Throughout MOISA 2 we worked closely with SRI to understand the functionality and architecture of IMDE/CSS and determine how the data from the three systems used in the Puget Sound could be integrated into IMDE and shared with the CSS widgets. With respect to Spillman, we were also able to attend a meeting of the Spillman Northwest User Group to understand how this organization worked alongside their users to enhance the Spillman system

as well as understand how users were applying Spillman technology within their agencies. Finally, we conducted telephone interviews with one expert user from each of the three systems used in the Puget Sound to understand how they were using the systems, their level of satisfaction with the system, and how the data from their systems could be utilized on the IMDE backbone (See Table **3** below for a list of key informants.)

Table 3: *Individuals contacted for Systems Analysis*

Name	**Title**	**Organization**
Ximena Avila	Director	SRI International
Anthony Dorsey	Field Sales Executive	Spillman
McCoy Smith	Area Client Services Manager	Spillman
Brady Walton	Support Department Supervisor	Spillman
Matt Jolly	Product Line Manager (Insight)	Spillman
Sgt Tobin Meyer	Supervisor, Boating Division, Sheriff (Spillman user)	Skagit County
Bob Pessemier	Project Consultant	WA-COP
Justin Theriot	VP, Delivery & Product Development	CommandBridge
Ed Madura	Security Director (CommandBridge user)	FSO, Port of Everett
Anne Tyler	Coast Guard Sector Puget Sound	Five Rivers Services, LLC
IS2 Dallas J. Shaw	HSIN Site Administrator (HSIN user and community creator)	DHS Joint Task Force West
Janusz Wasiolek	HSIN Mission Advocate Manager	DHS Contractor on HSIN

5.4 Overview

IMDE/CSS is a DHS S&T project to deliver enhanced situational awareness and information exchange across organizational boundaries. IMDE supports robust information sharing via data federation across agency boundaries while CSS provides information to aid in the existing concept-of-operations of tactical coastal surveillance and vessel interdiction. CSS improves the detection of uncooperative targets (i.e., threat vessels and aircraft) through persistent wide-area surveillance, automatic fusion, cue-able asset tasking, anomaly alerting, and strategic threat

targeting. IMDE/CSS integrates maps, cameras, and radar across multiple networks and uses a federated approach to facilitate the integration of existing enterprise service catalogs, registries, access control, systems and information.[39]

Spillman is a commercial product that began in 1983 as a law enforcement software program to manage records and information electronically. Spillman Technologies Incorporated is a privately held company headquartered in Salt Lake City, Utah with 250 employees. The Spillman software includes 46 fully integrated modules that allows users to perform such tasks as records management (RMS), computer-aided dispatch (CAD), mobile data and field reporting, mapping and GIS. It also includes over 2,000 preformatted reports.

Although Spillman was not initially developed for maritime users, Sergeant Tobin Meyer, Supervisor, Boating Division, Sheriff, Skagit County is currently using Spillman for land and maritime operations. In addition, as discussed in the MOISA 1 Final Report, maritime operations often necessitate coordination with entities that do not necessarily have a maritime focus. Sgt Meyer used funds from a Port Security Grant to have functionality (see Section 5.6 section below) added to various Spillman modules, which enhances its use for maritime operations. The original Investment Justification was developed and written with the aid of the Marine Exchange of Seattle Fiduciary Agent, Skagit County Sheriff's Office, and Skagit County Information Services. The partners on the project included, Spillman, Skagit County Information Services, Island County Information Services, San Juan County Information Services, and all local law enforcement agencies in Skagit County. Officer Rick Norrie, Coupeville Town Marshall, would like to receive similar maritime data via Spillman, but does not have required funding.

CommandBridge, is a commercial product developed by the Mariner Group in 2000 that provides situation management collaboration and coordination to the maritime community. In March 2015, the Mariner Group integrated CommandBridge as the core situational awareness system for the Washington Common Operating Platform (WA-COP). WA-COP is a secure, collaborative software platform for public and private maritime and related stakeholders to

[39] "Draft Coastal Surveillance System User's Guide" dated September 1, 2015

share information for decision making in support of the safety, security, and daily operations of the State of Washington ports and neighboring communities. In addition to CommandBridge, it includes five other component applications (see Appendix B:) to allow stakeholders to collect, share, and display multi-dimensional information for facilitation of collaborative planning and response to daily and emergency events, incidents, and threats. It is intended to be configurable for diverse users in a broad range of situations, providing a shared display of events and incidents on a map with applicable geographically referenced overlays and data enhancement. The CommandBridge dashboard will allow users to monitor status and activity in their areas of interest and then perform collection, analysis, and dissemination. Currently WA-COP has issued only 50 user licenses and, other than the CommandBridge component, is not a prominent system in the Puget Sound area; therefore, the remainder of this chapter will focus on an analysis of CommandBridge with brief overview of WA-COP functionality where appropriate.

HSIN is a DHS service that provides a SharePoint web portal system that allows federal, state, local, tribal, international, public, and private (FSLTIPP) sector agencies to share "Sensitive But Unclassified (SBU)" data over a secure channel[40]. It is operated by DHS and was first implemented in 2003 to replace the informal personal networks for information sharing that were in use at that time. HSIN is used to support event management operations by enabling real-time communications for emerging threats and incident response and helping intelligence analysts and public safety officials across the country to share information. For example, it has been used in response to the Boston Marathon bombing in 2013, Superstorm Sandy in October 2012, and the Deep Water Horizon Oil Spill in 2010. HSIN is also a SharePoint-based repository for archives and supports workflow processes.

5.5 User Base

IMDE/CSS's intended user base includes the United States Coast Guard (USCG), Customs and Border Patrol (CBP), and others in the FSLTIPP community who require a tool for maritime

[40] "Homeland Security Information Network". Department of Homeland Security (http://www.dhs.gov/homeland-security-information-network-hsin). Retrieved August 30, 2015.

domain awareness, targeting, planning, scheduling, execution, surveillance monitoring and management, and information sharing.

Spillman currently serves more than 1,400 agencies and nearly 70,000 public safety professionals in 41 states. Approximately 85% of Spillman users use the software to share data with anywhere from two to 51 other Spillman or non-Spillman agencies.

In the Puget Sound region, Spillman is used by law enforcement in Skagit, Whatcom, Island, and San Juan counties. As stated in the 5.4 Overview section above, Sergeant Tobin Meyer, Supervisor, Boating Division, Sheriff, Skagit County, used Port Security Grant Program (PSGP) funds to add real-time mapping capability to the Spillman system. With this modification, Sgt Meyer says he is able to see a common picture of an event in real-time, receive real-time updates, see all assets equipped with GPS in real-time, see pre-built GIS layers at will, and get weather updates etc. from/for all first response agencies in Skagit County including fire, law, and Emergency Management Services (EMS). The other major enhancement was a direct real-time link between Skagit County data and Island and San Juan County data so that they are able to receive real-time data about people, premises, vehicles, vessels, etc. as a land or maritime incident unfolds. This essentially links the northern Puget Sound together under one common data sharing system with the capability to link to all Spillman enabled agencies. With Spillman, Sgt Meyer says he is able to see in real-time where land and maritime assets are, how they are responding and receive real-time updates using the mapping module. He is able to activate or deactivate GIS layers at will that are in his GIS arsenal that includes virtually anything that would be relevant for a given event or ongoing events. The GPS tracking capabilities are onboard his patrol vessels, patrol cars, EMS, fire, and other equipped assets. Sgt Meyer states he is very happy with these upgrades to Spillman and as an incident commander is able to select the information he needs to make critical decisions. He further stated that he would find the system even more useful if other counties were added and he is interested in pursuing funding opportunities to integrate Blue Force Automatic Identification System (AIS) data into the Spillman mapping capabilities to push mapping information/GPS and GIS information to the JHOC.

CommandBridge has approximately 30 users from 16 agencies in the Puget Sound region who are using CommandBridge via WA-COP. The Washington State Ferry System, the Washington State Fusion Center, Washington State Parks and Recreation, and the Port of Everett Security use it.[41] Outside of WA-COP, CommandBridge operates in just under 50% of all tier one US ports, including Hawaii and Puerto Rico and has been contracted by the Pentagon to provide them with alerts.[42]

Ed Madura, the Security Director for the Port of Everett since 2008, uses CommandBridge via WA-COP for vessel tracking and alerting functions. He finds the ability to set trip wires for vessel alerting particularly useful. He does not use the CommandPost iPhone application within CommandBridge because he does not have any assets underway; however, he would use it if he did. He has been a user of CommandBridge for several years and finds the system easy to use. CommandBridge also provides him with AIS feeds. The CommandBridge software platform architecture also allows other sensor feeds, such as cameras, radar, sonar, access control and alarm systems, to be ingested and displayed. Madura has cameras on a closed network and shares a limited number of feeds with the Coast Guard and would like to receive camera feeds that are owned by the Coast Guard, but does not need that data on a daily basis. These cameras are not accessed through CommandBridge.

HSIN has 50,300 registered users as of August 21, 2015. Those using HSIN include police officers and firefighters; information officers; intelligence analysts; fusion center directors; Homeland security advisors; emergency management directors; police security officers; critical infrastructure planners and risk analysts; and custom and border patrol agents. In 2014, over 1,100 users logged in each day to support operational requirements, while 1,200 new users joined HSIN each month to access resources.

Petty Officer Dallas Shaw, USCG, who is currently working on a special project in San Antonio, is a daily community creator of HSIN. Shaw uses HSIN in daily operations to make timely and informed decisions as well as to identify courses of action during an event or threat situation. Looking up contingency plans and incident management reports for other sectors is

[41] Provided by Bob Pessemier, WA-COP Project Coordinator via email on 10 September 2015
[42] Provided by Stephen Dryer, President & CEO of The Mariner Group on 21 September 2015

also a function that Shaw uses regularly. In addition, Shaw uses HSIN Box, the HSIN secure messaging platform, and "in an ideal world" would prefer that everyone use HSIN for email message exchange as it would provide secure and trustworthy messaging capability with one point of login entry. Shaw also uses HSIN Alerts to manage his daily and future activities and accesses the DHS Common Operating Picture (COP) via HSIN.

5.6 Functionality

The following six top-level capabilities[43] were identified as required in the IMDE/CSS system in order to close the capability gaps outlined in the department's small vessel security strategy (SVSS) implementation plan:

1. Tracking: Tactically relevant and persistent domain awareness (people, vessels, cargo) sharable up to FOUO/LES Unclassified level with the capability to detect and persistently monitor maritime activity to include cooperative and non-cooperative vessels; identify, query and filter vessels of interest automatically based on user-defined criteria; and differentiate multiple track types/classes (i.e., air and maritime).
2. Data Fusion: Information sharing at up to FOUO/LES Unclassified level across appropriate Homeland Security Enterprise (HSE) law enforcement, intelligence analysts/joint operators/senior decision makers/interagency offices with the capability to view, customize and disseminate appropriate operational and intelligence information and data as well as to store and retrieve appropriate operational and intelligence information and data.
3. Planning and Execution: Unified DHS operations planning and execution suite that will allow users to monitor real-time operations; perform pre-mission risk-based planning and scheduling; adjudicate, coordinate and execute operations; perform post-mission analysis and documentation; and assess operational resources capability and availability.

[43] IMDE/CSS Requirements List-Draft-031115.xls provided by Mark Miller on March 27, 2015.

4. Alerting: Automated alerting that would allow users to conduct queries across multiple data sources and sensors, alert other agencies to vessel and/or area of interest, generate and send alerts based on user-defined criteria; and define alerting criteria based on models of abnormal behavior (e.g., loitering off a high-interest area).
5. Authorization: Authorized access based on standard user attributes and proper handling of agreed content markings with the capability to manage access, distribution, and control of information; manage persistent user attributes and credentials for FSLTIPP users; and provide compliance with applicable federal laws, executive orders, management directives, management instructions, policies, regulations, standards, and guidance.
6. Dashboards: Browser-agnostic User-Defined Operational Picture (UDOP) and interface interoperable with existing situational tools (e.g., C2, INTEL). UDOPs are quick dashboards of vital information that allow users to make fast, accurate decisions. The IMDE/CSS UDOP will be designed to be customizable for each user/operator.

This section evaluates how/if these capabilities are implemented in the three systems in operation in the Puget Sound (see *Figure 2*: Summary of required functional capabilities) and provides an overview of the systems' other capabilities.

Spillman's integrated suite of 46 software modules (see Appendix B: for a brief description of each of these modules) is designed for use by public safety agencies. The key components include a single-source database, master tables, Geographic Information System (GIS) technology, and message center. Master tables allow users to enter data once, where it is automatically shared among related modules. Related files can be attached to records, including images, audio files, and other essential documents.

Master tables include names, vehicles, property, wanted persons, on-call scheduling, demographic summary, resources, and dissemination. Searching the local database as well as state and national databases for up-to-date records and images is provided. When information is queried, integration with the Spillman database allows warnings or alerts associated with the record to appear in red to notify personnel of potential danger. Users can also access detailed

information about hazardous materials, their location, and recommended treatment so personnel can respond safely and with the knowledge necessary to perform their jobs.

The Spillman GIS technology is integrated into Spillman's CAD and CAD Mapping modules, which provide automatic notification of warrants, alerts, and past criminal incidents associated with an address. Reverse geocoding is also available. When coordinates are entered, the software displays a list of matching addresses. Search of multiple map layers is also available, including common places such as parks, bodies of water, address points, parcels, and streets. To provide GIS functionality, Spillman integrates with Esri's ArcGIS Server.

Sgt Meyer uses the CAD modules of Spillman to perform daily dispatch activities. He is able to see calls in real-time (by the hour or minute), see land and maritime assets as they are dispatched, and receive alerts when new data is added. While Sgt Meyer has sensors, which he can see in a real-time map view, he does not have access to sensor data on assets in other counties. However, this access could be made available via the Insight tool (see Data Fusion Section 5.10).

Although the Spillman software does allow users to monitor operations in real-time and do in-the-moment planning for things that are happening right now, it does not currently include mission planning or blue force data. According to Sgt Meyer, the integration of blue force data into the Spillman system would be especially useful, as it would allow him to access multiple sources of information from one point of access. He described a recent incident in which there were three agencies responding, but because they did not have an integrated planning, scheduling, and execution tool, they all dispatched overlapping assets. Having access to a common planning, scheduling, and execution tool along with the ability to see asset location on a map view could greatly increase efficiency and mitigate the risk of "blue-on-blue" in dangerous conditions.

Spillman does not have a browser-agnostic UDOP nor is its interface interoperable with any situational awareness tools without additional development and enhancement by Spillman. (See Entitlement and Identity Management section 5.9 for a description of authorization capabilities and the Data Fusion section 5.10 for details on how information sharing functions in Spillman.)

CommandBridge supports ingestion and visualization of dynamic data from sensors, cameras, radar, sonar, access control and alarm systems, employing user-defined rules, alerts and workflow to detect anomalous track behavior and assist with incident response. Over the past year, the Mariner Group has added the following new features: oil plume modeling, air traffic monitoring, vessel routing, personnel tracking, and escorting. A recent major update to CommandBridge also enables customers to enhance their network and cyber security. The new cyber integration safeguards digital assets through a combination of machine-based learning and human monitoring.

As used in WA-COP, *CommandBridge* offers the following top-level capabilities:

1. AIS vessel tracking
2. Status and activity monitoring for AIS transmitting vessels
3. Incident command
4. Resource tracking and management

CommandBridge does not provide a unified planning and execution suite; however, the Wrike tool (see Appendix B:) available as part of WA-COP is an online task and project management platform to help stakeholders manage day-to-day and emergency tasks, projects or incidents that could be used for planning, scheduling, and execution. CommandBridge provides a browser-agnostic UDOP (accessible from http://pswacop.org) that provides a quick link to the other five WA-COP applications (see Appendix B:) and allows users to see a real-time and historical view of events and activities in the region. However, this dashboard is not interoperable with any other situational tools without additional development and enhancement. (See Entitlement and Identity Management section 5.9 for a description of authorization capabilities and the Data Fusion section 5.10 for details on how information sharing functions in CommandBridge.)

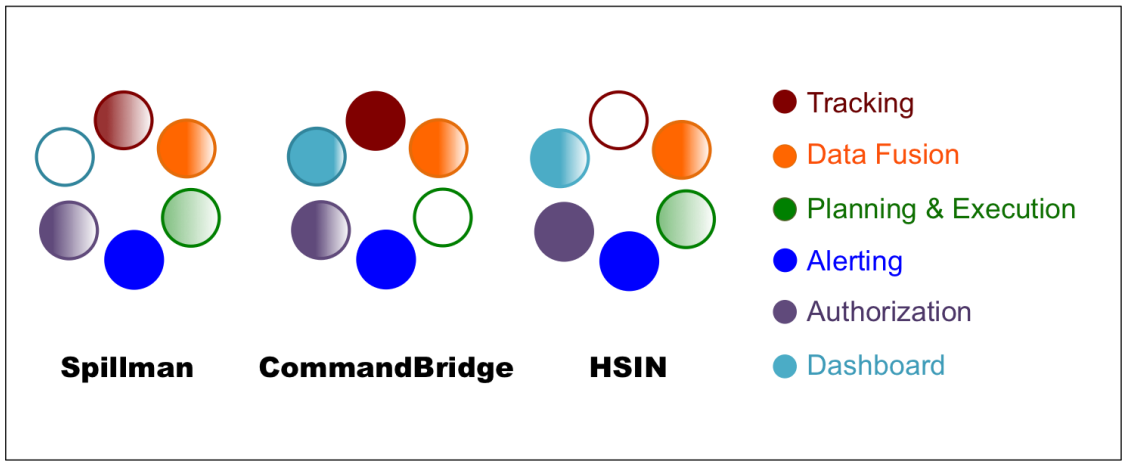
HSIN offers the following features and capabilities:

1. Alerts and notifications: While HSIN does not offer alerts of suspicious activity, it can pass along alerts generated by an external capability and sent by that external activity to a user via HSIN email and text capabilities.

2. Basic learning management system: Online training for HSIN and Community of Interest (COI)-specific training.
3. HSIN training: Self-paced computer-based training designed to help users understand how to use HSIN features and build/maintain a COI.
4. Document repository: Allows documents to be categorized, accessed and posted in real-time. Offers version control, check out features, and notifications of changes.
5. GIS mapping: Geospatial mapping capabilities that allow sharing of geographical data from various sources on one display; mapping of incident scenes and planned events; tracking of movements/changes over time; and viewing of weather-related information.
6. Instant messaging (HSIN Chat): Provides a secure environment for instant messaging that allows real-time information sharing one-on-one or in groups.
7. Managed workflow capabilities: Routes documents from lists and libraries to individuals to request a response, assign tasks, gain approvals, and collect feedback and signatures.
8. Secure messaging (HSINBox): Secure emails can be sent to mission partners or managed distribution lists. Documents, links and notes may be attached.
9. Web conferencing (HSIN Connect): Provides a secure environment for real-time conferencing, web-based training, and large-scale webinars using voice, audio, and video.

Although HSIN provides many useful capabilities and is used throughout the Puget Sound, some capabilities were seen as either lacking or difficult to use. IS2 Shaw reported that while GIS mapping capabilities are available in HSIN and he does use them, these are static displays only. HSIN has no capability to generate, store or display dynamic moving tracks. In addition, Sgt Meyer from Skagit County finds HSIN cumbersome to navigate and very difficult to filter out irrelevant data. HSIN also does not provide a unified planning and execution suite. (See Entitlement and Identity Management (Security) section 5.9 for a description of authorization capabilities; Data Fusion section 5.10 for details on how information sharing functions in HSIN.)

Figure 2: Summary of required functional capabilities



5.7 Mobility Solutions

CSS includes the user interface portion of the IMDE/CSS system. It is a web application and as such, has a component that runs in the browser that interacts directly with the client. This client application uses HTML5, which has many features for supporting mobile devices (e.g., cell phones and tablets) included. The CSS development team is aware of the need to provide services to users using a variety of tools and anticipates providing mobile friendly services as new CSS features are developed.

Spillman Mobile allows users to access maps, up-to-the-minute call details, and records (including name, property, vehicle and incident records) on laptops and mobile devices. The Spillman Mobile modules allow personnel to see alerts on names, vehicles and addresses, view the location of other field officers, and maintain constant communication with dispatchers and other units. Sensitive data is transmitted over a secure wireless connection instead of a radio frequency where unauthorized parties may overhear it. Mobile's Instant Messaging provides individual windows for chat conversations and allows personnel to build custom groups of users and instantly see who is busy, offline, or available for chat.

As a Boating Supervisor for Skagit County and incident commander, Sgt Meyer uses the Spillman Mobile mapping feature for response coordination to monitor how units (human resources, land vehicles, maritime vessels) are responding, their location, and all active calls.

He also uses a laptop with touch screen from a vehicle or vessel to perform searches on license plates or vessel registrations to determine if the vehicle or vessel has been involved in illegal or suspicious activity.

CommandBridge has an iPad/iPhone/Android app named CommandPost that lets mobile users share their position and post brief status messages to the CommandBridge Docking Well. It also allows mobile users to view all the same tracks, alerts, zones and situations available to full CommandBridge users over WiFi or 4G connections. It also has a mobile friendly web site, enabling users to access the application functionality using the web browser on their mobile device. As mentioned in the User Base Section 5.5, Ed Madura has access to CommandPost, but does not use it because he does not have any assets underway.

HSIN mobile access is available for the HSIN Connect (virtual meeting and desktop sharing) application. iOS and Android support for the SharePoint portion of HSIN is more limited due to browser compatibility issues tied to the Microsoft SharePoint 2010 platform. Compatibility is tested against common Internet browsers, primarily Internet Explorer and Firefox.

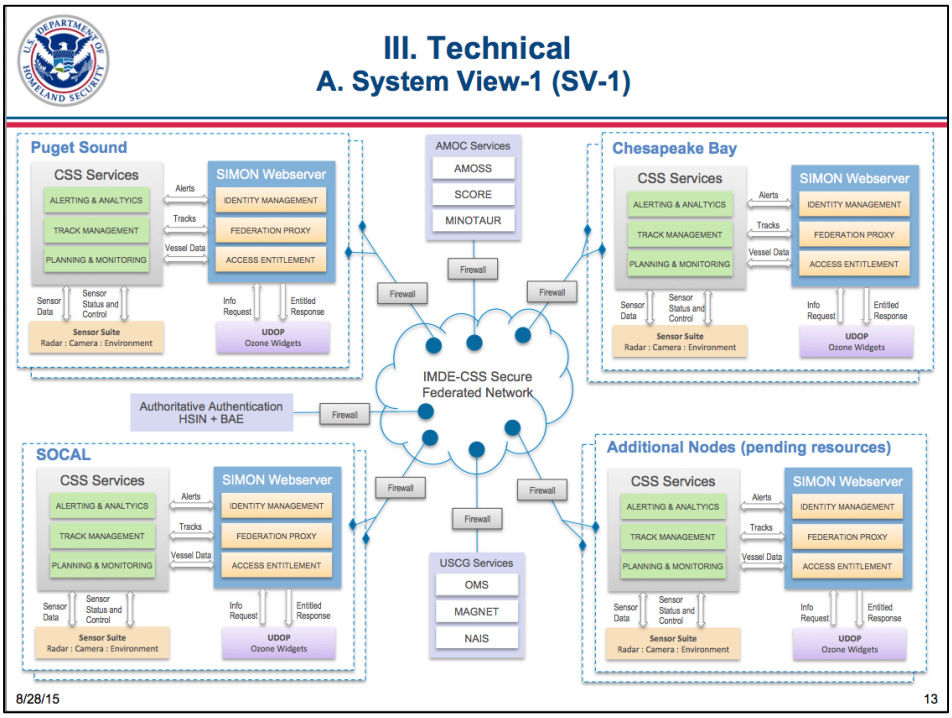
5.8 Architecture

The *IMDE* architecture allows data to be read from FSLTIPP sensors of various kinds. It is designed to also read and write data on operations and planning. The CSS component combines these data feeds into operationally relevant views that can be configured by the users to aid them to understand the evolving situations they are handling. The goal is to allow system owners to share information with whomever they want, when they want (see *Figure 3*).

The IMDE/CSS application uses a services oriented architecture pattern, which supports information sharing between different types of systems by exposing modular interfaces between the different types of applications. In general, such information sharing requires some amount of work, both at the technical and business levels. At the business level, the different entities need to agree on what will be shared, how the data will be protected and the business case for the effort. At the technical level, there is generally work to implement the specific

interfaces on one side or the other. If one of the applications has been built to provide a specific service (such as a SQL database engine or an authentication server) the work will be mainly on the service user. For the case of IMDE/CSS connecting to any of the applications considered here, there will be work on both sides. Part of this work may be writing code to put data that is being transmitted into National Information Exchange Model (NIEM) or Common Alerting Protocol (CAP) format. This is discussed in more detail in the Data Fusion section below.

Figure 3: Technical System View of IMDE/CSS[44]



Spillman has a three-tier architecture, with a SQL database persistence layer, a sophisticated server-side business layer and a variety of client-facing applications, including standalone Windows applications and a web interface (InSight Browser based client). Spillman is developed using UNIX and Windows-based technologies as well as industry standards such

[44] IMDE CSS Intro toSector_PugetSound_20150816.pptx provided by Joe Campillo on August 16, 2015

as Extensible Markup Language[45] (XML) and Open Database Connectivity[46] (ODBC). Spillman's interfaces allow information to be shared between Spillman and many common third-party software vendors, including IMDE/CSS, using the industry-standard NIEM. Spillman does not exchange alerts in the CAP format.

CommandBridge has a three-tier architecture, with a SQL database persistence layer, a sophisticated server-side business layer along with a web application and iOS/Android client-facing layers. The server hardware can be hosted at Mariner's cloud hosting solution or be physically located at the client's site or a combination of the two. The client may want to host the application locally for security concerns or to address latency issues. It is possible to have data pre-processed at the client site, then to forward the data packets to the cloud host for storage. CommandBridge does not exchange alerts in the CAP format.

HSIN is an instantiation of a SharePoint web application platform (based on SharePoint 2010). The HSIN architecture has the potential to be highly complex. SharePoint is a web application platform in the Microsoft Office server suite. Launched in 2001, it combines traditionally separate applications such as intranet, content management, document management, enterprise search, business intelligence, and workflow management.[47] In general,

---

[45] Retrieved from Wikipedia on May 11, 2015: **Extensible Markup Language** (**XML**) is a markup language that defines a set of rules for encoding documents in a format, which is both human-readable and machine-readable. It is defined by the W3C's XML 1.0 Specification and by several other related specifications, all of which are free open standards. The design goals of XML emphasize simplicity, generality and usability across the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures such as those used in web services. Several schema systems exist to aid in the definition of XML-based languages, while many application programming interfaces (APIs) have been developed to aid the processing of XML data.

[46] Retrieved from Wikipedia on May 11, 2015: **ODBC** (**Open Database Connectivity**) is a standard programming language middleware API for accessing database management systems (DBMS). The designers of ODBC aimed to make it independent of database systems and operating systems. An application written using ODBC can be ported to other platforms, both on the client and server side, with few changes to the data access code.

[47] "SharePoint 2010 Overview Evaluation Guide" (PDF). Microsoft Corporation. 7 May 2010. Retrieved August 30, 2015.

SharePoint follows the three-tier architecture model, with hooks to Windows functions and applications (especially Office products), using SQL Server for the database engine.

5.9 Entitlement and Identity Management (Security)

Each of the four systems under consideration has a way to ensure that only people who present the proper credentials are allowed access to the system. Once allowed onto the system, individual users can be granted or denied access to particular resources depending on the configuration of resource and user attributes. These functions are known as authentication and authorization.

Authentication is the "login" process – it uses some credentials (usually username and password) provided by the user to establish that the user is the person they claim to be. Authorization refers to granting or denying access based on user attributes.

Identity management refers to the entire process of allowing or denying access to system resources. It includes authentication and authorization, as well as other necessary functions.[48] Entitlement can be taken to mean the fine-grained control over access, that is, authorization.

Authorization can be implemented using role-based access control (RBAC) or attribute-based access control (ABAC). In RBAC, the decision for access is based on whether the user belongs to some particular group. In ABAC, the decision is based on whether the user has (or doesn't have) some set of attributes. ABAC is often viewed as a more powerful strategy, especially in complex environments such as sharing data among agencies. The data source for the user attributes can be decoupled from the authentication server, which could be an advantage if agencies use a single source for authentication (for example, HSIN) and other source(s) for attribute server(s), such as an application that is local to the particular agency.

A Project Interoperability in Puget Sound (PIPS) initiative is starting in October 2015 at the University of Washington that will further investigate the requirements for identity, credential, and access management (ICAM) in shared systems (federated authentication and authorization), their current use among the maritime community in Puget Sound, and

[48] https://en.wikipedia.org/wiki/Identity_management#System_capabilities

opportunities for future ISE enhancements through initiatives like IMDE/CSS. To the extent that the needs of the community in Puget Sound are common to similar communities in other geographic regions, the findings of this initiative can be generalized to inform national development and maintenance of ICAM systems.

As for the four systems of interest here:

IMDE/CSS uses HSIN or BAE Systems, Inc. Identity and Access Management for the authentication server and attribute-based authorization. BAE Systems, Inc. is the US subsidiary of BAE Systems plc, a London-based defense, security and aerospace company which delivers a full range of product and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support services (http://www.baesystems.com/). BAE provides authentication and authorization software, as well as other specialized security and protection software solutions, for law enforcement and first responders.

This evaluation is considering IMDE/CSS as it could be developed (assuming time and funding) to be an application that could be deployed in an operational setting. Every such application must have a working solution for authentication and authorization. The Project Interoperability in Puget Sound initiative will support defining the authentication and authorization policies that need to be in place to provide a sufficient trust environment to enable the user community to be confident in the access that is enabled by IMDE/CSS.

Spillman enables agencies to manage security options for specific computers and users and keep a record of users who try to log into the system. Agencies can choose to require multifactor authentication before a user can log into the system from a computer. If an agency enables multifactor authentication, users must insert an authorized USB drive into the computer before a login can be completed. Spillman also offers encryption that complies with the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS).

CommandBridge uses role-based authorization and a Microsoft .NET security for authentication. Windows security policies are enforced at the client, service, and database layers. Encryption certificates and/or Virtual Private Network (VPN) solutions are used for

data transport across networks. Role-based access controls are also used to restrict access to applications or content within the system as deemed necessary by the client's system administrator.

HSIN uses an Oracle Identity Management stack to handle its authentication. Sharepoint 2010, hence HSIN, supports claims-based authentication that provides the ability to exchange attributes as part of the data available to the application receiving the login data. The set of attributes available is not yet standardized. The IMDE/CSS team is working with the HSIN team to develop the set of attributes that IMDE/CSS will need to support the policies identified by the PIPS initiative.

HSIN provides fine-grained control over the data in the database. The data owner must grant access to users for them to be able to access it. Not all links within the HSIN site point to data sources within HSIN (e.g. RISS Secure Intranet (RISSNET) is an external application). Logging into HSIN can provide a login to linked applications such as RISSNET using a single sign on process. This can greatly simplify the authentication process because the user doesn't have to sign in multiple times to multiple applications.

HSIN uses a two-factor authentication for access, which is a security feature that requires you to provide two forms of identification to log into the system. When accessing HSIN, the main screen asks you to log in with a username and password. You will then be asked to elect a delivery method for the system to send a one-time passcode to your email address or phone number via text message or recorded message. You will need to enter this passcode within 10 minutes to access HSIN. This enhanced security feature confirms identity and maintains the integrity of the network.

5.10 Data Fusion

IMDE is designed to be able to read data streams from other applications via any of a set of protocols (SOAP, REST or JMS queues). It can also export data to other applications via the same set of protocols. Because IMDE is able to pull data from a variety of sources, it is also possible to integrate the data sources into a coherent view, thus adding value to the individual

streams by connecting data elements that would otherwise have to be connected manually by the users. Pulling data from external sensor systems and showing it within the CSS desktop web application is an example of data fusion.

The various information sources accessible through IMDE can be thought of as "widgets" that can be shown within a "dashboard" on the computer desktop. The widgets can be part of the CSS module, or they can be web applications from other sources (e.g. the Spillman InSight web application). To put external web applications onto the dashboard, the application web code is "wrapped" in boilerplate code that is sent to the client. For example, the CSS Planning and Scheduling widget could combine information from different agencies such as their available assets.

To perform data fusion with any of the specific applications considered here will require additional work beyond any that is planned in any detailed manner in the current IMDE/CSS roadmap. In general, the data could travel from the IMDE/CSS pipeline to the external application. This would probably be a new type of data for the external application. The company developers would need to build the code to accept the data feed and the UI to display it. Conversely, the data could travel from the external application to IMDE/CSS. The IMDE/CSS developers would need to build the code to accept the data and probably the UI to show it. In either case, it could be valuable to combine the data feed with other data to form a melded package. Also, the identity management/security aspects of the data need to be addressed. The end user must have authorization to see the data. If it is stored on either side, the requirement authorization data must be stored with it. In general, the data can be transmitted in NIEM or CAP formats, given some level of programming effort.

Spillman provides interoperability through its *Insight* product. *Insight* allows multiple participating agencies, including those using disparate software systems, to connect databases. This model allows each agency to search for information outside its jurisdiction and receive critical up-to-date information. To share data with other agencies using Spillman, a search can be sent directly to a central message switch, which then routes the search request in real time to the other agencies connected to *InSight*. If one or more agencies have data matching the search criteria, the information is returned to the requestor through the central broker. For agencies

that do not use Spillman, a browser-based client is available to make queries and receive responses entirely from the Web-based application. No client software is required to be installed or downloaded to a workstation. This tool uses Asynchronous Java and XML (AJAX), allowing the browser to maintain a seamless look and feel while data is transferred between the browser and the *Insight* broker. Spillman uses the National Information Exchange Model (NIEM) to interface with third party systems.

CommandBridge exports data to the end user. This data may come from different agencies, enabling CommandBridge to function as a portal to data from multiple agencies.

HSIN participates in federations with other federal systems that enable the interchange of data and information. A federated database system is a type of meta-database management system (DBMS), which transparently maps multiple autonomous database systems into a single federated database. Through these federations, interoperability is achieved between HSIN and other federal systems.

5.11 Licensing/Maintenance/Training/User Groups

IMDE/CSS will be available to users free of charge.

Spillman software is sold as a single site license agreement rather than individual user licenses, allowing agencies to have an unlimited number of users on the system at no additional software expense. Spillman offers a Grant Assistance Program that provides agencies with help finding and applying for grant funds. A dedicated Spillman grant specialist will help agencies write grant applications and meet federal and state grant requirements. They also offer public safety financing options, allowing agencies to spread the cost of their software systems over several years while benefitting from low interest rate, tax-exempt payment methods. Agencies must pay an annual maintenance fee that covers the cost of live 24/7 customer support, upgrades, and enhancements to the licensed software.

Both on-site and off-site training and education is available for new and existing users. Off-site training occurs at regional Spillman offices as well as at a 4-day annual user conference with instruction and demonstrations of current products and incoming innovations. Online

training is available for commonly used modules. Regional user groups have been organized to provide users with the opportunity to share ideas, discuss problems, vote for enhancements and find solutions to common issues.

CommandBridge can be accessed by Puget Sound community members free of charge via WA-COP, which is funded by a port security grant. Users interested in CommandBridge can request a login. An extension for Phase 2 of WA-COP, which ended August 31, 2015 has been requested. Funds for training and support are also being requested under the port security grant.

HSIN training is available free of charge for all users to include state/local/tribal/territorial (SLTT) partners such as fusion centers, emergency management offices, and police departments for use supporting the homeland security mission. It is also available for federal use primarily for coordinating across federal departments and agencies, or with SLTT homeland security partners. Training includes common software applications; specific modules on SharePoint elements and system component training – such as the how to use the Lightning Conductor capability. Training is live via webinar (Connect) or static in computer-based modules.

There are no maintenance costs. HSIN's help desk is accessible 24/7 through email and telephone providing individuals support through text and voice communication. Individuals with access and functional needs can request additional support and may be directed to work with a HSIN Mission Advocate (HSIN's "field team") to provide accommodation.

Each community of interest (COI) has a HSIN mission advocate (MA) who serves as the primary point of contact for HSIN users; providing customer support, training and outreach. Each MA is assigned a specific area of responsibility (AOR) based on their mission experience and technical expertise. IS2 Shaw believes that the MA is an important concept and that any system needs this kind of infrastructure in order to succeed.

5.12 Opportunities and Constraints

The desire to integrate operations and data across the maritime community is one that has been identified by all levels across the FSLTIPP community. In the Puget Sound region, the community has begun to use some private systems (e.g., Spillman) and some government sponsored systems (e.g., HSIN) to integrate operations and share data; however, a federated system such as IMDE/CSS could allow entities to connect and manage their individual web applications in a single operating environment, thereby reducing the number of systems that larger Federal agencies have to keep track of and further encouraging interagency operability across the region. Through the upcoming technical and operational demonstrations of IMDE/CS, DHS hopes to build momentum for the implementation of such a system in the Puget Sound and across the nation.

The design philosophy of the IMDE/CSS software development team is to use an agile process[49] to build tools that meet identified user needs. Agile management, or *agile process management*, or simply *agile* refer to an iterative, incremental method of managing the design and build activities for engineering, information technology, and other business areas that aims to provide new product or service development in a highly flexible and interactive manner. In partnership with MOISA, the IMDE/CSS development team at SRI is employing a distinctly human-centered Agile approach, but the Agile process is used by many software teams without a robust human-centered design methodology.

Critical problems in software development can arise from a disconnect between the potential user community and the development team. A tight, agile team of software developers, human centered designers, and operational professionals can provide a much tighter feedback loop during design and build iterations. This allows frequent course correction, increasing the chances that the system will meet user needs, and that users will accept the software because it addresses their real pain points and they have been given some ownership during the design phase. The agile development process as a whole increases the odds that the software can be built on time and within budget by minimizing the number of

[49] https://en.wikipedia.org/wiki/Agile_management

false starts. The human centered aspect of the development processes maximizes the odds that the software will be usable, useful and appropriate for the operating environment.

MOISA 2 has helped initiate such a human-centered, agile, iterative design and development process for the IMDE/CSS project through a collaboration between the University of Washington Human Centered Design & Engineering Department and SRI International (the IMDE/CSS developer).[50] MOISA 2 researchers have built on the connections to the community developed during MOSIA 1 as well as the insights into their current ISE (e.g. that this particular community depends heavily on personal relationships and face-to-face interactions). Sections 7 and 8 provide additional detail on the MOISA 2/SRI collaboration in support of IMDE/CSS.

Another important opportunity for IMDE/CSS is that its enterprise architecture can leverage existing mature systems already in use within the maritime community, such as those discussed here (see *Figure 3* above). The ability that IMDE provides to integrate the data from these mature systems results not only in a cost savings to the entire FSLTIPP community, but also improves the adoption of IMDE/CSS by providing users with access to the systems with which they are already familiar. In addition, the Internet browser agnostic user-defined interface that is proposed for CSS allows users to customize their desktop to complement their workflows; adding both CSS widgets as well as the mature systems they are already using to give them one entry point for all their daily tasks.

Finally, IMDE anticipates using HSIN for authorization and authentication, an already proven, single sign-in capability that allows the community to share data. IMDE is also working on a centralized attribute store for use in policy creation that will enhance the identity and access management capabilities of the system. Authentication at the attribute level (i.e. entitlement) will allow users to share information with trusted partners on an individual mission and/or incident occasion.

As described here, there are many opportunities and challenges surrounding the technical aspects of the current Puget Sound ISE, particularly in the context of a demonstration

[50] Note that IMDE office is not yet committed to funding the FY16 continuation of the agile process recommended by this report.

of a regional enterprise architecture. During the lead-up to planned demonstrations of IMDE/CSS in 2016, the UW and SRI team has built momentum for a CSS Planning and Scheduling widget that would include demonstrating the IMDE data fusion capabilities and use of the ICAM layer. By taking advantage of regional trusted partnerships and the momentum being built for IMDE/CSS, we have the opportunity to increase situational awareness and information sharing capability that will enable FSLTIPP partners to better accomplish their safety, security and resilience operations.

6 Use Cases

A major thrust of MOISA's second year research consisted of a detailed analysis of the business process and technical aspects of two use cases. The use cases studied were (1) the detection, tracking and recognition of small vessel suspicious activity and (2) operational planning and scheduling. The results of the analysis on the two use cases are presented below.

6.1 Classification of Suspicious Small Vessels – Use Case #1

6.1.1 Motivation

Small vessels are defined as "any watercraft – regardless of method of propulsion – less than 300 gross tons used for recreational or commercial purposes. Small vessels include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other small commercial vessels involved in foreign or US voyages."[51] The National Marine Manufacturers Association (NMMA) estimated that in 2014 there were over 12 million of these boats registered in the US.[52] Small vessels require little training and/or licensing to operate, are relatively affordable, and operate close to critical infrastructure and under the expectation of little regulation. Most small vessels are not required to carry automatic identification system (AIS) equipment and are therefore largely anonymous.[53] In practice for the maritime law enforcement and safety community, "small vessel" means vessels not transmitting AIS or signals commonly used to track ocean going vessels.

Consequently law enforcement agencies face the challenge of distinguishing between the vast number of legitimate small vessel operators and the comparatively few individuals who are estimated to be engaged in illicit activities.[54] The Department of Homeland Security is

[51] DHS. (2011). Small Vessel Security Implementation Plan Report to the Public.
[52] Boat Sales Strong with Summer on the Horizon. (2015). Retrieved August 27, 2015, from http://www.nmma.org/news.aspx?id=19879
[53] USCG Navigation Center. (2015). AIS Requirements. Retrieved April 26, 2015, from http://www.navcen.uscg.gov/ ?pageName=AISRequirementsRev
[54] GAO. (2013). Maritime Security: DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy. GAO-14-32.

concerned that small vessels, due to their anonymity, could be used to ``smuggle terrorists or weapons into the United States, as a stand-off weapon platform, or as a direct attack method to deliver a water-borne improvised explosive device (WBIED).''[55]

Small vessels have been used for military or terrorist purposes several times in the past. Small vessels were used in the 1980s Tanker War when the Iranian Naval Revolutionary Guard fired missiles, guns, and rockets at larger vessels (mostly tankers) from small boats.[56,57] In more recent times, the Iranian Revolutionary Guard Corps Navy (IRGCN) has acquired the Bladerunner speedboat in an attempt to build a fast attack craft fleet with the goal of controlling the Strait of Hormuz.[58] A small vessel was also used in the high profile bombing of the USS Cole in 2000 in the Port of Aden, Yemen.[59] In 2002, al-Qaeda attacked the M/V Limburg in the Arabian Sea with a small suicide boat, killing a crew member and damaging the ship.[60] If an attack damaged a major transportation corridor or port terminal in the US, the economic impacts could reach into the billions.[61]

An additional small vessel threat is the use of these vessels to smuggle drugs across the northern US border. A recent example occurred on 29 August 2015, when a Taiwanese citizen was discovered importing drugs into the United States via a small vessel near the San Juan

---

[55] Department of Homeland Security. (2011). Small Vessel Security Implementation Plan Report to the Public. Retrieved from http://www.dhs.gov/xlibrary/assets/dhs-uscg-small-vessel-security-strategy-report-to-public-012011.pdf

[56] While little damage was inflicted to the hull and/or cargo, during the attacks the insurance premium for vessels transiting the Gulf increased by as much as 50%.

[57] Times, E. S., Special to The New York. (1987, September 3). From Air and Sea, Iran-Iraq ``Tanker War'' Heats Up. The New York Times. Retrieved from http://www.nytimes.com/1987/09/03/world/from-air-and-sea-iran-iraq-tanker-war-heats-up.html

[58] Baker, B. (2013, January). Iran's fast attack craft fleet: behind the hyperbole. Retrieved from http://www.naval-technology.com/features/featureiran-fast-attack-craft-fleet-behind-hyperbole/

[59] Naval History and Heritage Command. (2001). Terrorist Attack on USS Cole: Background and Issues for Congress. Retrieved from http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/t/terrorist-attack-on-uss-cole-background-and-issues-for-congress.html

[60] http://www.globalsecurity.org/security/profiles/limburg_oil_tanker_attacked.htm accessed 9/22/15

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

Islands.[62] From 2005 to 2010, Washington state ranked first in the nation for federal seizures of MDMA.[63] The Puget Sound area is classified as a High Intensity Drug Trafficking Area (HIDTA) by the Office of National Drug Control Policy due to the fact that "the Strait of Juan de Fuca represents the longest continuous US international maritime border. Many parts of this region are remote, while others have an extremely high density of small vessel traffic. Smuggling of marijuana, MDMA, and cocaine occurs in this region, and guns and money flow across the border in exchange for drugs."[64]

MOISA research has noted several cooperative efforts among actors throughout the federal, state, local, tribal, international public and private (FSLTIPP) maritime community to improve maritime domain awareness with the goal of enhancing local, regional, and national security through information sharing and cooperation. The August 2015 MDMA drug seizure, for example, was a result of a cooperative effort by the US Coast Guard, US Customs and Border Protection, Homeland Security Investigations, Royal Canadian Mounted Police, and the Bellingham Police Department. Below is a review of the current small vessel security and safety operations conducted by select maritime actors in the Puget Sound region.

6.1.2 Objectives and Definitions

The goal of this small vessel security use case is to understand the role of the local law enforcement community in Puget Sound in addressing the small vessel threat. The objectives of the use case are to determine how local law enforcement (1) detects, (2) identifies, and (3) responds to small vessel threats.

---

[62] 53 pounds of MDMA seized from boat near San Juan Islands. (n.d.). Retrieved from http://www.seattletimes.com/seattle-news/crime/53-pounds-of-ecstasy-seized-from-boat-near-san-juan-islands/

[63] Based on dosage unit. Executive Office of the President, Office of National Drug Control Policy. (2010). High Intensity Drug Trafficking Areas Program Report to Congress.

[64] Testimony of Dave Rodriguez Director, Northwest High Intensity Drug Trafficking Area (HIDTA) (22 April 2015). Prepared for the Committee on Homeland Security and Government Affairs "Securing the Border: Understanding the Threats and Strategies for the Northern Border." Pg. 12.

6.1.2.1 Detect

In this use case, 'detect' means to become aware of the presence of a vessel, its location, and the vessel's suspicious nature or behavior. All three pieces of information must be present for detection to be complete. Two different scenarios are included in this definition: (1) law enforcement becomes aware of a vessel exhibiting suspicious behavior and its location through sources, such as sensors or other boaters and (2) a marine patrol is physically on scene with a boat that is behaving suspiciously. The detection is not satisfied only by having knowledge that a suspicious vessel is expected in the future without its actual location; although a "be on the lookout" (BOLO) or all-points bulletin (APB) may contribute to the objective of identification, it does not qualify as detection.

6.1.2.2 Identify

To identify a vessel means to learn who the owner is and the vessel's hull identification number (HIN) and Washington state registration number (WN), if applicable. If a BOLO or APB includes the vessel owner or WN/HIN, it would meet the definition of identifying the vessel.

6.1.2.3 Respond

Response is any action taken after detection and includes reaction to both suspicious and non-suspicious vessels. For example, a routine safety check is a response to a detected non-suspicious vessel. Identification does not need to occur before a response takes place; identifying the vessel can be a form of response. To respond could mean to pass on information, to withdraw from the situation, to surveil, to interdict, etc. The definition of "respond" is intentionally broad.

6.1.3 Methods

To discover and characterize local small vessel security operations, we attended community meetings, conducted formal face-to-face interviews with select members, and reviewed published literature and related resources. Interviewees for the face-to-face interviews were

selected from agencies that represented local law enforcement in the counties that border the northern section of Puget Sound and the Strait of Juan de Fuca. To identify candidates for interviews, we worked with an Interagency Operations Center (IOC) liaison based at the US Coast Guard, Sector Puget Sound to develop a list of desirable organizations to interview. Interviews[65], each lasting approximately 1 hour, were conducted with

- Clallam County Sheriff's Office
- East Jefferson Fire Rescue in Jefferson County
- JeffComm 9-1-1 Communications in Jefferson County
- Jefferson County Sheriff's Office
- King County Sheriff's Office Aviation Support Unit
- King County Sheriff's Office Marine Rescue and Dive
- Skagit County Sheriff's Office
- Snohomish County Sheriff's Office
- US Drug Enforcement Agency
- USCG Sector Puget Sound
- USCG Station Seattle
- Whatcom County Sheriff's Office

Information obtained from MOISA year 1 interviews is also included. The relevant interviews were with

- Bainbridge Island Police Department
- Customs and Border Protection Office of Air and Marine (OAM) - Bellingham, WA
- Port Gamble S'Klallam Tribe, Natural Resources
- USCG Auxiliary
- Washington Department of Fish and Wildlife

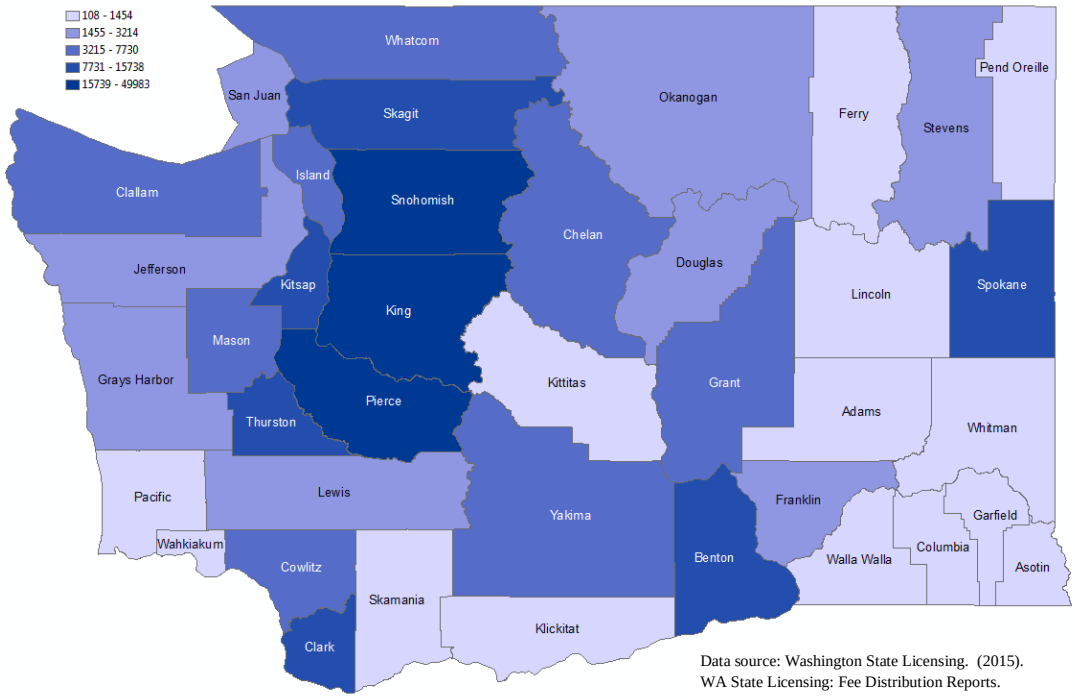
Meetings that were attended include a Washington State Ferry active shooter exercise, and the sensor workshops that are described in Section 4. Document review includes sources from Washington Parks and Recreation, USCG, DHS, and CBP, among others.

[65] This list only includes structured interviews conducted in support of use cases and does not include community events, which included a larger group of participants, such as the Sensor Survey Workshop.

6.1.4 Results

The geographical area that the small vessel security use case focuses on includes the counties that border Puget Sound and the Strait of Juan de Fuca, specifically: Clallam, Jefferson, King, Island, San Juan, Skagit, Snohomish, and Whatcom. In fiscal year 2014, there were 241,280 registered vessels in Washington State. In the relevant counties, there were 105,635 registered vessels (see *Figure 4*).[66]

Figure 4: Vessel Registration by County, Fiscal Year 2014



Vessel registration is filed under the owner's residence which may not be where the boat is operated. The vessel registration fees are distributed to counties according to the number of vessels registered in each county.

[66] Washington State Licensing. (2015). WA State Licensing: Fee Distribution Reports. Retrieved August 9, 2015, from https://fortress.wa.gov/dol/vsd/vsdFeeDistribution/DisplayReport.aspx?rpt=2014F99-09.csv&countBit=0

6.1.4.1 Safety

Small vessels require little training and/or licensing to operate; are relatively affordable; and operate under the expectation of little regulation. These conditions result in the potential for a high number of boating safety violations. Examples of boating safety rules include using correct navigation lights, following the International Regulations for Preventing Collisions at Sea (COLREGS), operating the vessel in a sober state, having the appropriate number of life jackets onboard, and maintaining a safe speed. In 2014, there were 122 accidents that resulted in 22 fatalities, 44 non-fatal injuries, and over $2 million in damages in Washington.[67]

The enforcement of local, state, and federal safety regulations on the water is the responsibility of the maritime law enforcement community. Marine patrol units in Washington State are funded in part by the USCG Marine Patrol Federal Financial Assistance Grant Program that is administered through the Washington State Parks and Recreation Commission, Recreational Boating Safety Program. The programs Application and Guidelines document states that, "under this grant program, the purpose of a marine patrol unit is to enforce RCW 79A.60 Regulation of Recreational Vessels. At our foundations, we are an injury prevention program. As such, we seek to work with our partners in law enforcement to reduce recreational boating injuries and accidents."[68] A second source of funding comes from Vessel Registration Funds (VRF). Missions paid for by VRF can only be for enforcing boating safety. The economic slowdown has led to fewer people buying and registering boats; this also reduces the overall VRF budget. The sheriff's offices and USCG officers that participated in this study report that recreational boating safety is their primary mission: For example:

- **Bainbridge Island Police Department:** The purpose of patrols is to make the boating experience safer.[69]

[67] USCG. (2015). 2014 Recreational Boating Statistics. Retrieved 24 August 2015, from http://www.uscgboating.org/library/accident-statistics/Recreational-Boating-Statistics-2014.pdf
[68] Washington State Parks and Recreation Commission. (2015). Recreational Boating Program Federal Financial Assistance Grant Program: Applications and Guidelines.
[69] MOISA interview with Bainbridge Island Police Department conducted 20 March 2014.

- **Clallam County Sheriff's Office (CCSO):** "The mission of the Sheriff's Marine Patrol Unit is to promote boater safety through education, enforcement, and active patrol of all waterways located in and around Clallam County."[70]
- **Jefferson County Sheriff's Office (JCSO):** The Sheriff Marine Patrol has "an aggressive policy [that] emphasizes safety of the boating public by enforcing the laws dealing directly with safety equipment and safe boat operation…The marine unit is dedicated to its primary mission of increasing boating and water safety."[71] A Jefferson County Sheriff's Office Deputy stated that, in the absence of an obvious violation, their reason for contacting a vessel is safety and education purposes.[72]
- **Whatcom County Sheriff's Office (WCSO):** "The marine patrol unit utilizes several vessels to enforce water safety laws on the various bodies of water within Whatcom County."[73]
- **Skagit County Sheriff's Office:** In an interview with the Skagit County Sheriff's Office, the deputy reported that the focus of his patrols is recreational boating safety.[74]
- **Snohomish County Sheriff's Office:** "The marine missions of the sheriffs and other local law enforcement are paid for through VRF [vessel registration fund] for the mission of boating safety.[75]
- **USCG Auxiliary:** "Our primary mission is recreational boating safety."[76]
- **USCG Station Seattle:** In an interview, a Station Seattle officer reported that recreational boating safety is the main job.[77]

  On the other hand, a few agencies identified their primary mission to be environmental or security rather than safety:

---

[70] Clallam County. (2014). Sheriff – Boating Safety 11003.811.
[71] Jefferson County. (2000). Marine Patrol. Retrieved 24 August 2015 from http://jeffersonco-treis.info/PDF%20Files/3.12%20Public%20Services%20References/Marine%20Patrol.pdf
[72] MOISA interview with Jefferson County Sheriff's Office conducted 6 February 2015.
[73] Jeff_Parks. (2011). Get on Board with the Marine Unit. Retrieved from http://www.whatcomcountysheriff.org/2011/05/16/get-on-board-with-the-marine-unit/
[74] MOISA interview with Skagit County Sheriff's Office conducted 28 May 2015.
[75] MOISA interview Snohomish County Sheriff's Office conducted 28 May 2015.
[76] MOISA interview with USCG Auxiliary conducted 7 May 2014.
[77] MOISA interview with USCG Station Seattle conducted 20 April 2015.

- **Port Gamble S'Klallam Tribe, Natural Resources:** Primary job is to protect fish and wildlife on water and land.
- **Customs and Border Protection (CBP):** Maritime security is 100% of what we do.[78]
- **Sector Puget Sound Enforcement Division:** Responsible for ensuring waterway security and safety including Waterside Operations Management; Law Enforcement; Ports, Waterways, and Coastal Security (PWCS).[79]

6.1.4.2 Security

Although different agencies view their primary duties differently, diverse elements of the FSLTIPP come together to address security issues. For example, although sheriff's offices see their duties as primarily safety related and CBP views security as its primary mission, several sheriffs join together with CBP to enhance border security in the Puget Sound region by conducting joint patrols. Although safety is the primary concern for the overwhelming majority of the non-federal actors, they contribute to a maritime community that often works in cooperation with the federal elements to address security concerns and incidents.

6.1.4.3 Detection

The primary method of detection and recognition of suspicious activity is marine patrol. Most entities that were interviewed for this study reported that they rarely, if ever, encounter a suspicious small vessel. Clallam County Sheriff's Office, for example, reported that out of the approximately 800 boats they contacted in the past year, only 1% were of a suspicious nature in a security sense. Marine patrols do, however, often encounter vessels that are not in compliance with regulations and not operating safely. Just among recreational crabbers "it's not uncommon to find violations on 50 to 80 percent of the boats we stop," said marine officer Eric Olson with WDFW.[80]

---

[78] MOISA interview with CBP conducted 19 December 2013.

[79] http://www.uscg.mil/d13/sectpugetsound/response/ accessed 9/22/15

[80] Welch, Craig. (21 August 2011). "Putting the pinch on illegal crabbers | The Seattle Times." Retrieved August 12, 2015, from http://www.seattletimes.com/seattle-news/putting-the-pinch-on-illegal-crabbers/

In Canada, the RCMP is focused upon maritime security issues, while in the US the primary agency with security responsibility is Customs and Border Protection. As described in Section 6.1.4.3.8 below, there is already exploratory sharing of RADAR data between the US and Canada and discussion about additional opportunities for increased information sharing and cooperation related to small vessel tracking in the neighboring waters of Puget Sound.

6.1.4.3.1 Patrol Resources

US marine patrols are carried out by various vessels owned by the USCG, the state, and the counties. See Table 4.

Table 4: *Select Puget Sound Marine Patrol Resources*

Entity	**Resources**
Bainbridge Island Police Department	33-foot vessel
Clallam County Sheriff's Office	One freshwater vessel – Boston Whaler; One saltwater vessel - 26-foot *Protector* with radiation detection equipment, 3-D Furuno radar, mobile data terminal, radar tower; 2 – 4 crewmembers
CBP OAM	Interceptor Class, Coastal Enforcement Class, and Riverine Class vessels
East Jefferson Fire Rescue	One 33-foot boat with FLIR; One 21-foot boat
King County Marine Unit	4 vessels (21-foot to 38.5-foot range) and 4 smaller vessels
Jefferson County Sheriff's Office	One 24-foot *Integrity*
San Juan County Sheriff's Office	4 vessels
Skagit County Sheriff's Office	33-foot SAFE Boat; min, 3 crewmembers
USCG Station Seattle	Three 41-foot utility boats, two 25-foot RB-HS, and two 25-foot RBS; all have radar and encrypted AIS
Whatcom County Sheriff's Office	Several vessels

6.1.4.3.2 Patrol Areas

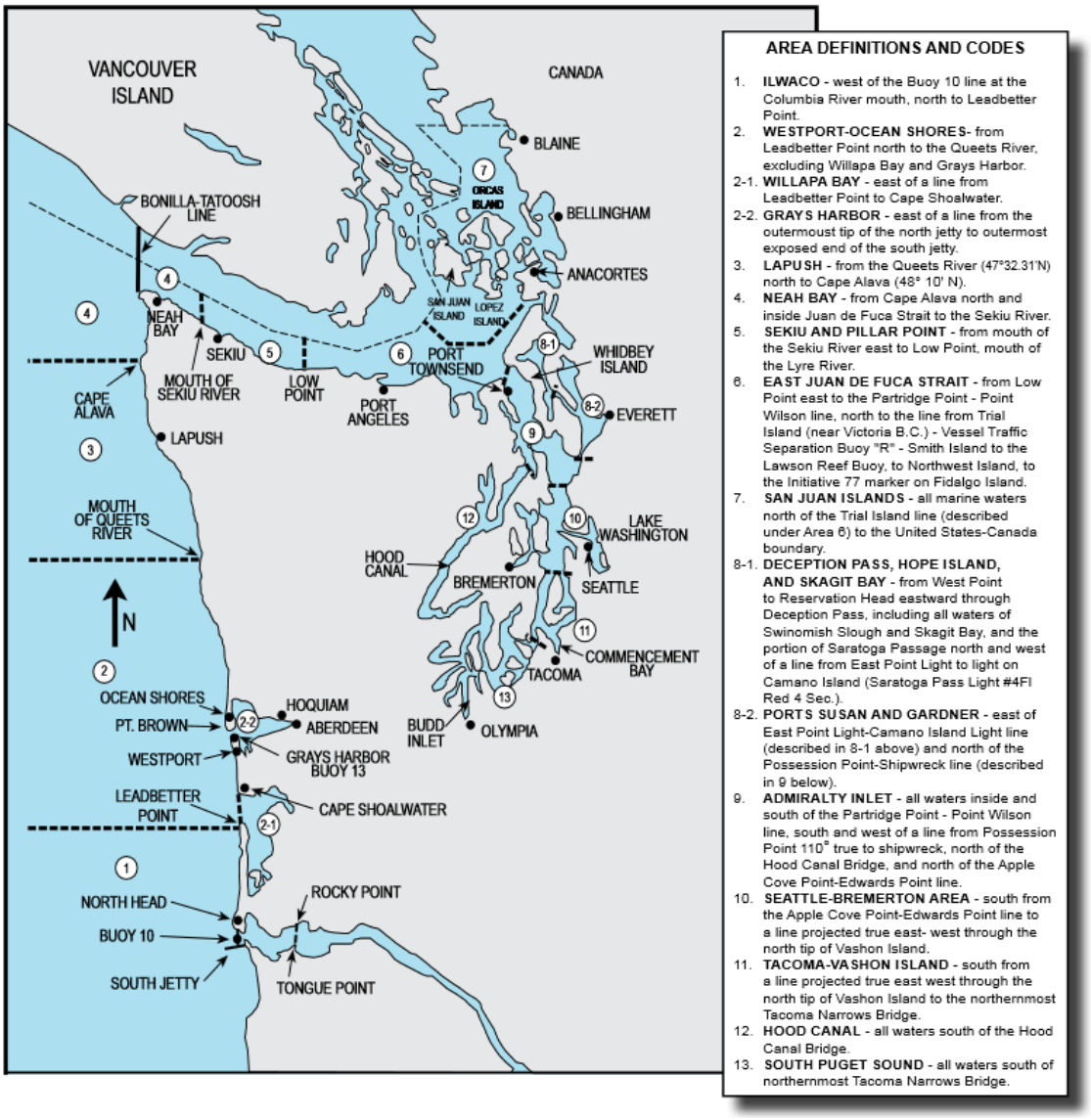
One key basis for choosing which area to patrol at a given time are the Washington Department of Fish and Wildlife (WDFW) marine areas (see *Figure 5*). Marine areas dictate which species are in season for fishing, the type of equipment that is allowed, and other special rules (e.g., motorboats prohibited).[81] Patrols will go to the marine areas that are expected to be the busiest based on the fishing season and/or the marine areas that are closed to detect vessels that are fishing illegally.

Open fishing areas can be large and encompass several counties. When a fishing area includes Clallam and Jefferson County, the sheriff's offices will coordinate their patrols before the season and communicate on the water to avoid duplicate contacts with vessels using cellphone, radio, and Blue Force Tracker (BFT) information. USCG does no fishing enforcement in Puget Sound since the areas are all state fisheries; it does enforce fishing regulations offshore. USCG will notify state/local authorities if they observe a suspected fishing violation in state fisheries. KCSO said it is more important to know where USCG is than where small vessels are.

[81] WDFW. (2015). Washington Sport Fishing Rules.

Figure 5: Marine Areas defined by the Washington Department of Fish and Wildlife.

Marine Areas defined by the Washington Department of Fish and Wildlife.



Source: WDFW. (2015). Washington Sport Fishing Rules. Pg. 103.

USCG Station Seattle chooses the location of patrols based on personnel requirements; each crewmember must patrol each area of the area of responsibility (AOR) twice every six months – one day patrol and one night patrol in each area. Other than this requirement, the location of patrol is random. USCG reported that there are no "hot spots" that require additional attention.

Whatcom County, which borders Canada and the Strait of Georgia, focuses its marine patrols on lakes (specifically Lake Samish and Lake Whatcom) that are popular recreational boating sites in the summer.

6.1.4.3.3 Patrol Times

Generally, sheriff's offices patrol only on weekends during peak boating seasons. This is due to the limited number of qualified marine officers/volunteers. During the off-season, CCSO will conduct two random patrols per month. East Jefferson Fire Rescue does not patrol but has two vessels on standby 24/7. The USCG patrols both day and night year round.

6.1.4.3.4 Joint Patrols

Clallam County Sheriff's Office (CCSO) has an MOU with CBP Border Patrol. The joint CBP-CCSO program runs part-time during the year; during that time CBP officers will join CCSO patrols 80-90% of the time. When CBP joins the CCSO patrol, CBP pays for wages and fuel. During a joint patrol, CBP activities include conducting immigration interviews, boarding, and reviewing paperwork. If CBP makes contact with a vessel making entry to the US during a patrol, that vessel is still required to report to a port of entry for an in-person declaration of entry (see Section 6.1.4.4.3 for more information). Whatcom County Sheriff's Office used to have a marine deputy embedded with CBP full-time year-round; now the program only runs five months out of the year.

The Washington Department of Fish and Wildlife does joint patrols with CCSO and WCSO. Every time CCSO goes out on patrol, they call WDFW to extend an invitation to join; WDFW joins nearly all of the time. CCSO and WDFW have a friendly arrangement and take each other's needs into consideration when determining where to patrol. WDFW has an MOU with the Port Gamble S'Klallam Tribe; WDFW will occasionally join S'Klallam patrols to aid in enforcement since tribal enforcement has no jurisdiction over non-tribal people.

Sector Puget Sound reported that there are very few notifications from state and local authorities to the USCG with regards to a small vessel. Sector Puget Sound does not work with local authorities in counter-drug operations; JCSO reported that they only occasionally work

with the USCG. The USCG relies on federal (including DEA, ICE, CBP, and DHS Investigations), rather than local, intelligence in their counter-drug efforts.

6.1.4.3.5 Shiprider

The United States and Canada participate in a joint maritime security activity named Shiprider. The program involves vessels jointly crewed by US and Canadian law enforcement officers, each authorized to enforce the law on both sides of the international maritime border. Working together, Canadian and US law enforcement officers are able to transit the maritime border to help secure it from national security threats, as well as counter cross-border smuggling and trafficking. Shiprider enforcement activities include detecting, monitoring, and boarding vessels in Canadian or US waters.

Vessels operated by the Royal Canadian Mounted Police (RCMP) and participating in the Shiprider program have a member of the USCG on board. The RCMP vessel is able to enter US waters to enforce US laws under the supervision of the USCG representative onboard. Similarly, USCG Shiprider vessels have a member of the RCMP on board and are able to enter Canadian waters to enforce Canadian laws under the supervision of the RCMP officer.

6.1.4.3.6 Suspicious Behavior

When on patrol, law enforcement officers reported considering the following questions in determining whether or not a small vessel is suspicious:

- Are unauthorized persons inappropriately trying to gain access to vessels or facilities?
- Is the size of the vessel's crew not typical for the type of small vessel?
- Are crew members reluctant to leave a vessel while it is being serviced and/or are they taking unusual security measures?
- Is a vessel anchored or running without lights in the dark?
- Are there smaller vessels hovering near a larger vessel?
- Are crew members recovering items from, or tossing items into, the water or onto the shoreline?

- Are vessel owners reluctant to fully identify themselves to a marina or harbor authority? Is it hard for those authorities to locate the owners?
- Is there unusual diving activity?
- Is the vessel avoiding law enforcement?
- Is the vessel in violation of boating safety/registration rules?
- Is the vessel hanging right off the border between the US and Canada?
- Are the crew members dropping pots as patrol approaches?
- Is the vessel fishing when nothing is in season?
- Does the vessel have out of state registration?
- Has the vessel been reported by other boaters?
- Is the vessel not abiding by a traffic separation scheme?
- Is the vessel operating erratically?
- Is the vessel seaworthy?
- Does the boat have correct fishing equipment?
- Is the vessel fishing in the correct area?
- Is a recreational vessel out in hazardous weather?

Although questions like these might suggest a template for suspicious boat activity, the DEA stated that a template or guidance on suspicious small vessels loses its usefulness for them because there is a constant game of adjusting to the other side's reactions.

Clallam County officers are authorized to do fishery inspections and do not need probable cause to search a vessel for the purpose of finding illegal fish or equipment. CCSO has no targeting method; they will talk to every vessel they encounter. CCSO stated that they do not need or desire any more sensor data to conduct their mission, but BOLO or other indicators of potentially threatening boats would be welcome. However, the Clallam Sheriff receives little, if any, information about threats from the Puget Sound Area.

6.1.4.3.7 Use of Sensors during Patrol

CCSO uses an onboard Furuno 3D radar only when visibility is low; they can find a 14-foot skiff a mile out. CCSO does not rely on radar to select vessels for boarding because the radar does not provide enough information to allow them to determine if they have already boarded a

vessel. CCSO also has an onboard computer and a Furuno Navigation Plotter on which they view radar and AIS. CCSO has indicated an openness to the possibility of sharing their onboard mobile sensor data with the Puget Sound security and safety community, as long as the equipment and sharing process did not cost CCSO any resources.

CCSO is a participant in the Puget Sound Radiation and Nuclear Detection Program. As a Type II participant, CCSO has the additional capability of conducting radiation/nuclear scans using a Radiation Solutions, Inc. (RSI) system. The system scans a vessel that is alongside the patrol boat, sends the information to Washington, D.C., and will alert the crew if there is a positive reading. CCSO reported that they were in need of no additional sensor data from other organizations.

6.1.4.3.8 Other Sources of Information

Sensor Detection

USCG Station Seattle's primary method of detection of small suspicious vessels is the Joint Harbor Operations Center (JHOC), who dispatches them to investigate unusual behavior. The Vessel Traffic Service (VTS) will also dispatch Station Seattle if they detect a vessel not abiding by the traffic separation scheme, however, USCG VTS radar does not have the ability to detect small vessels; its mandate is to provide safety services to large commercial vessels.

Presently, select US VTS radar (e.g., Cape Flattery) provide data to Canada's Marine Communications and Traffic Services (MCTS), which is able to refine the information using a SIGNALIS processor to detect small boat operations. Canadian VTS sites also leverage this capability to detect both large and small vessels. USCG Sector Puget Sound reported that Canada can share its VTS information with USCG but, due to the high level of resources involved in sharing the information on an ad hoc basis, only does so in exercises and on a case-by-case basis. There is currently no formal ongoing real-time data flow occurring, and the process of passing the data in on a case-by-case basis requires increased personnel commitments on the Canadian side of the border for the duration of any sharing demonstration.

SIGNALIS is a joint French/German system that automatically tracks many vessels, analyzing for behavior such as speed, heading, history, meeting, and border crossing location. The system generates alarms for the operators, allowing for plotting of interception courses and tracking of target vessels. The operators can program the system to generate alarms based on a wide variety of available information. The system allows for analysis of data over time to provide intelligence and to support deployment of resources. This system is used by the Royal Canadian Mounted Police to monitor the movement of small vessels in the Salish Sea.

Bulletins and Meetings

Law enforcement- and intelligence-derived information of potential small vessel threats is shared through various semi-formal meetings and email bulletins distributed across the region's maritime community. USCG Station Seattle receives monthly messages from the El Paso Intel Fusion Center (EPIC) National Lookout List. County sheriffs receive information from regional bulletins that may include information on vessels of interest or BOLOs.

Classification causes an impediment to information sharing in the region. The Washington State Fusion Center (WSFC) receives both classified and unclassified information, but it has no authority to sanitize or declassify information. As there is a very limited number of personnel cleared to receive classified information in the maritime security community, the amount of intelligence passed from federal agencies to state and local law enforcement through WSFC is very small.

In the past, USCG Station Seattle held Quarterly Information Exchange meetings, but the meetings are no longer held due to increased operation requirements. CCSO, USCG, WDFW, and Port Angeles Border Patrol occasionally meet as the Intel Group to discuss operations and what types of boats are of interest. Again, this information does not amount to detection, but it does aid in patrols' ability to detect suspicious vessels. Several organizations referenced the Area Maritime Security Committee (AMSC) as a source of information.

6.1.4.4 Identification

6.1.4.4.1 Registration

A vessel operating in US waters will either be a state registered vessel, a federally documented vessel, or a foreign vessel. A state registered vessel must have a registration card onboard whenever the vessel is on water and must display their registration number and decal on the vessel's bow.[82] A federally documented vessel – a vessel nationally registered with the United States Coast Guard rather than with a state – must have the vessel name and hailing port visible somewhere on the hull.

In Washington, recreational vessel owners must register their vessel with the Washington State Department of Licensing (DOL) with the following notable exceptions:

- Vessels under 16 feet powered with less than 10 horsepower used on waters with no federal jurisdiction,
- Human-powered vessels,
- Documented charter vessels,
- Vessels used exclusively for racing,[83] and
- Tribal vessels used in the exercise of treaty fishing rights that are tribally registered.[84]

Documented vessels must still register with the state and display the registration decal but are prohibited from having and displaying a Washington registration number.[85] Vessels used exclusively for commercial fishing and documented vessels used primarily for commercial purposes receive two decals: one annual decal from the DOL and one permanent decal from the Department of Revenue (DOR). The DOR levies a personal property tax on these vessels.[86]

---

[82] Washington State Recreation and Conservation Office. (2009). Boating Regulations in Washington State. Retrieved from http://boat.wa.gov/regulations.asp

[83] WAC 308-93-030: Vessels subject to excise tax, registration and titling exemptions. (n.d.). Retrieved August 9, 2015, from http://app.leg.wa.gov/wac/default.aspx?cite=308-93-030

[84] WAC 308-93-720: Indian tribe exempt vessels. (n.d.). Retrieved August 10, 2015, from http://app.leg.wa.gov/wac/default.aspx?cite=308-93-720

[85] Washington State Department of Licensing. (n.d.). Vessel Numbering Instructions. Retrieved August 9, 2015 from http://www.dol.wa.gov/forms/420082.pdf

[86] Department of Revenue. (2015). Commercial Vessel Tax. Retrieved August 9, 2015 from http://dor.wa.gov/docs/pubs/industSpecific/Vessel.pdf

Generally a county sheriff's deputy will only run a registration number if something about the vessel and/or people aboard piques their interest (see Section 6.1.4.3.6). Registration numbers from any US state can be searched by law enforcement officials. CCSO reported that they cannot run the number onboard; instead they ask dispatch over the radio. Dispatch then messages the result to the patrol boat's onboard computer. Documented vessels can be looked up online via the NOAA Fisheries Office of Science and Technology website by name[87] or by identification number.[88] For example, if you look up the Washington State Ferries vessel Samish on the NOAA site, the returned result is seen in Figure 6. Incorrect registration raises suspicion; if a vessel's registration is not valid, law enforcement officials may issue a ticket or may take a closer look at the vessel. Additionally, counties that use the Spillman system (see Section 5) can check if a vessel operator has a valid Washington Boater Education Card.

Figure 6: The NOAA document vessel search result for WSF Samish

Vessel Name:	**SAMISH**
Vessel Service:	PASSENGER (INSPECTED)
Trade Indicator:	Coastwise Unrestricted
Hull Material:	STEEL
Ship Builder:	VIGOR FAB
Hailing Port:	SEATTLE WA
Owner:	WASHINGTON STATE FERRIES 2901 3RD AVE SUITE 500 SEATTLE, WA 98121
Documentation Issuance Date:	April 10, 2015
Previous Vessel Names:	No Vessel Name Changes
USCG Doc. No.:	**1251777**
IMO Number:	9720251
Call Sign:	WDH7552
Hull Number:	7102
Year Built:	2015
Length (ft.):	347.7
Hull Depth (ft.):	24.5
Hull Breadth (ft.):	83.3
Gross Tonnage:	3525
Net Tonnage:	3055
Documentation Expiration Date:	April 30, 2016
Previous Vessel Owners:	STATE OF WASHINGTON

6.1.4.4.2 AIS

Unlike large commercial vessels, small recreational vessels are not required to carry Automatic Identification System (AIS) equipment onboard. AIS is used by large vessels and certain

[87] www.st.nmfs.noaa.gov/st1/CoastGuard/VesselByName.html

[88] www.st.nmfs.noaa.gov/st1/CoastGuard/VesselByID.html

smaller vessels to broadcast their identity, location, speed, and heading in order to reduce the risk of collision. Any vessel is permitted to use AIS if the operator so wishes, but because most small vessels are not carrying AIS equipment they are largely anonymous. For local law enforcement officials like CCSO, when they encounter a non-commercial vessel, whether it is transmitting AIS is irrelevant. CCSO is focused on maximizing its on-water encounters rather than being vectored by suspicious activity detected by other sensors.

6.1.4.4.3 Alternative Inspection System

Another requirement that small vessels are generally exempt from in USCG District 13 is the submission of an advance notice of arrival. The only exception is if the small vessel is carry dangerous cargo.[89] Small vessels arriving from outside the US, however, must make a face-to-face application, via Customs Form 1300 Vessel Entrance, to lawfully enter the United States within 48 hours of making landfall.[90]

To be exempt from making an in-person application, a person must be a participant in an alternative inspection system programs, i.e., they must be participating in NEXUS, holders of a Canadian Border Boat Landing Permit, or operators using either the Outlying Area Reporting System or Small Vessel Reporting System. These exemptions still require an announcement of arrival via telephone to CBP,[91] and do not "preclude the requirement for physical reporting upon request by US Customs and Border Protection."[92]

NEXUS

---

[89] USCG. (2003). Title 33: Navigation and Navigable Waters PART 160—PORTS AND WATERWAYS SAFETY—GENERAL, Subpart C—Notification of Arrival, Hazardous Conditions, and Certain Dangerous Cargos

[90] 19 CFR 4.3 - Vessels required to enter; place of entry. | US Law | LII / Legal Information Institute. (2010). Retrieved September 2, 2015, from https://www.law.cornell.edu/cfr/text/19/4.3

[91] CBP. (n.d.). Pleasure Boat Reporting Requirements. Retrieved 24 August 2015 from http://www.cbp.gov/travel/pleasure-boats-private-flyers/pleasure-boat-overview

[92] Reporting Requirements for Recreational Vessels Arriving in U.S. along Lake Erie Shoreline | U.S. Customs and Border Protection. (n.d.). Retrieved August 25, 2015, from http://www.cbp.gov/travel/pleasure-boats-private-flyers/Reporting%20Requirements%20for%20Recreational%20Vessels%20Arriving%20in%20U.S.%20along%20Lake%20Erie%20Shoreline

NEXUS is a joint US-Canadian program that expedites participants' travel across the northern border. A NEXUS card is an approved alternative to a passport under the Western Hemisphere Travel Initiative and can be used at air, land, and marine ports of entry. The card is valid for five years. For the vessel to qualify for telephone-only entry, all crew and passengers must be members of a Trusted Traveler program.[93]

Canadian Border Boat Landing Permit

The Canadian Border Boat Landing (Customs Form I-68) Permit authorizes the holder to enter the US with no requirement to report in person to a CBP port of entry. The holder is required to be interviewed by CBP, photographed, fingerprinted, and allow their vessel to be initially inspected. The permit is valid for one year. For the vessel to qualify for telephone-only entry, all crew and passengers must be members of a Trusted Traveler program;[94] "when the I-68 is used by a person who is not a US citizen or lawful permanent resident of the United States, admission shall be for no more than 72 hours and only if they will remain in nearby shopping areas, nearby residential neighborhoods, or other similar areas adjacent to the immediate shore areas of the United States."[95]

Outlying Area Reporting System

The Outlying Area Reporting System is a northern border option for reporting entry into the US. This system uses videophones to allow CBP officials to speak to and see the person entering. The videophones are at select locations – usually public marinas.[96]

---

[93] NEXUS Program Description | U.S. Customs and Border Protection. (n.d.). Retrieved August 25, 2015, from http://www.cbp.gov/travel/trusted-traveler-programs/nexus/nexus-overview

[94] Canadian Border Boat Landing (I-68) Program | U.S. Customs and Border Protection. (n.d.). Retrieved August 25, 2015, from http://www.cbp.gov/travel/pleasure-boats-private-flyers/cbbl

[95] CBP. (2014). Reporting Requirements for all Private Boat Operators in Minnesota/North Dakota Boundary Waters.

[96] Reporting Requirements for Recreational Vessels Arriving in U.S. along Lake Erie Shoreline | U.S. Customs and Border Protection. (n.d.). Retrieved August 27, 2015, from http://www.cbp.gov/travel/pleasure-boats-private-flyers/Reporting%20Requirements%20for%20Recreational%20Vessels%20Arriving%20in%20U.S.%20along%20Lake%20Erie%20Shoreline

Small Vessel Reporting System

The small vessel reporting system (SVRS) is a voluntary web-based automated online reporting system. Participants are able to report intended international arrivals in advance of departure. Once the filer has filed a float plan, CBP will issue a float plan number which is used when telephonically entering the US to match the caller to the vessel.[97] Passengers of the small vessel who are not previously registered through the SVRS must still report in person.[98]

6.1.4.5 Response

State and local law enforcement have primary jurisdiction three miles offshore[99] and up to the Canadian border in the Strait of Juan de Fuca. Federal officials' authority extends to 200 miles offshore. Law enforcement officials have the authority to stop and board any vessel on Washington waters. Law enforcement officials can do safety and fisheries inspections without probable cause. WDFW Fish and Wildlife Officers (FWOs) hold commissions from the US Fish and Wildlife Service and NOAA's Office of Law Enforcement which gives them jurisdiction over specific federal violations, most importantly the Endangered Species Act and the Lacy Act.[100] FWOs also hold county commissions and can enforce county ordinances including boating safety laws.[101] As stated before, USCG does not do fisheries enforcement in Washington

[97] Federal Register | Agency Information Collection Activities: Small Vessel Reporting System. (2015). Retrieved August 25, 2015, from https://www.federalregister.gov/articles/2015/03/20/2015-06374/agency-information-collection-activities-small-vessel-reporting-system#h-9

[98] CBP Announces New Small Vessel Reporting System. (n.d.). Retrieved August 24, 2015, from https://www.dvidshub.net/audio/27282/cbp-announces-new-small-vessel-reporting-system

[99] RCW 43.143.005

[100] Under the Lacey Act, it is unlawful to import, export, sell, acquire, or purchase fish, wildlife or plants that are taken, possessed, transported, or sold: 1) in violation of U.S. or Indian law, or 2) in interstate or foreign commerce involving any fish, wildlife, or plants taken possessed or sold in violation of State or foreign law. USFWS (n.d.). Lacey Act. Retrieved September 2, 2015, from http://www.fws.gov/international/laws-treaties-agreements/us-conservation-laws/lacey-act.html

[101] Under the Lacey Act, it is unlawful to import, export, sell, acquire, or purchase fish, wildlife or plants that are taken, possessed, transported, or sold: 1) in violation of U.S. or Indian law, or 2) in interstate or foreign commerce involving any fish, wildlife, or plants taken possessed or sold in violation of State or foreign law. USFWS (n.d.). Lacey Act. Retrieved September 2, 2015, from http://www.fws.gov/international/laws-treaties-agreements/us-conservation-laws/lacey-act.html

waters. USCG will also often let local law enforcement handle boating under the influence (BUI) offenses since the state ticket is more expensive than the USCG ticket.

6.1.4.5.1 Boardings

Vessels do not need to be behaving suspiciously to warrant contact by law enforcement. USCG Station Seattle reported that sometimes they will board everyone that has not been boarded in the last 6 months. Sometimes Station Seattle uses a quota system (e.g., six boardings per day), but that approach is not always effective. Occasionally a quota approach will result in stopping a suspicious vessel, but most of the time it does not. Considering that each time USCG boards a vessel, the USCG asset is tied up for a long period of time, a preferred method is to stop vessels based on intelligence reports or indicators of suspicious activity (see Section 6.1.4.3.6).

If a Station Seattle patrol decides to board a vessel they will call back to the station to inform them that they are transitioning a team. If the vessel is suspicious, the crew will ask those onboard approach questions and conduct an administrative checklist based on the size of the vessel. They will visually inspect the boat and run the names of the people onboard. The names are run through the National Targeting Center to check if there are any warrants in effect. The USCG has access to the For Official Use Only (FOUO) database Maritime Information for Safety and Law Enforcement (MISLE) which has records of every incident that a vessel has been involved in. If the USCG finds something criminal aboard the vessel, such as illegal drugs, the operational chain of command goes through the JHOC.

Counties do not have access to MISLE; they can access the Port State Information eXchange (PSIX)[102], which contains weekly information that has been released through the Freedom of Information Act (FOIA). County law enforcement generally tries to correct noncompliance through education rather than tickets.

[102] https://cgmix.uscg.mil/PSIX/Default.aspx

6.1.4.5.2 Fire Department Response – Example Case

East Jefferson Fire Rescue (EJFR) provides a striking example of the complex protocol, practices, and practicalities involved in a response situation. For EJFR there are three categories of vessels that require response: (1) vessels in distress, (2) vessels requesting assistance, and (3) suspicious vessels. Vessels are assumed to be in the first two categories unless identified as suspicious by customs or law enforcement. Regardless of the category, the procedure is the same:

1. Law enforcement will get the call first because the USCG does not have a local station.
2. Calls generally come through the local Public Safety Answering Point (PSAP) 9-1-1 Call Center, Jefferson Communications (JeffCom); USCG sometimes calls directly.
3. A shore-based response is sent to the point of last vessel sighting where a command post (CP) is established. An "Eyes-On Station" (EO) establishes eyes on the vessel – not the same person, but in the same geographic space. The EO's job is to maintain visual contact with the vessel at all times. USCG will pass information to them. EJFR leans on air assets from USCG in Port Angeles and has them use FLIR. EJFR has FLIR on their new boat, but the camera elevation is only 9.5 feet high, limiting the range to 12 miles. The detection of the vessel is always visual. The boats have RADAR, but it is not used to find vessels since the wave height is usually too high. If the wave height is not too high, RADAR is still not generally used since everyone onboard is too busy. The helmsman spends his time getting "from point A to point B". The Coxswain is also the radio operator. The EO is multitasking, too.
4. A line of bearing is determined from the shore-based visual ID point.
5. Another ground asset is sent to get a cross bearing to fix the position of the vessel; sometimes that cross bearing is provided by Central Whidbey Fire Rescue.
6. In a "go" situation – the vessel location has been determined and EJFR decides to respond – EJFR will send two marine assets to assist.

   EJFR uses the following guidance to determine if a situation is go/no-go. If any one of the following items is not met, then it is a "no-go" situation.

   a. It is a life threatening situation or the vessel is in immediate distress.

b. The weather conditions (wind, waves, tide) are not unsafe – Jefferson County is in a unique situation with regard to weather, tides, currents, and winds. The weather conditions can change from fair to storm very quickly and without warning. EJFR boats are not called on in conditions that are unfavorable.

c. A legitimate crew must be available – A certified coxswain is the ultimate decision maker on whether the boat goes, but not all marine personnel are coxswains. EJFR does not use USCG training because it is designed for fair weather conditions. EJFR uses Canadian Coast Guard training for safety and operations at sea. Many crewmembers are volunteers. Therefore, it is possible that when a call comes in the personnel are not present to form a legitimate crew. Travel time to the launch site can be lengthy for volunteers that live far away. Water events take approximately 2 hours; if another call comes during those two hours, there will not be a crew (or boat) available.

d. A second marine unit is available – EJFR requires an additional marine unit be present to act as a rescue platform for the primary marine unit. Law enforcement will go with one unit only, if necessary. Central Whidbey Fire Rescue (CWFR) is a partner with EJFR; CWFR has a 16-foot rigid-hulled inflatable boat (RHIB). The Clipper ferry and Washington State Ferries have assisted before.

e. Vessel is not suspicious – The marine unit is not armed. If anything on the boat they are approaching looks suspicious they will abort the mission and notify USCG.

All the above conditions must be met in order to launch a marine unit. The conditions have been influenced by elected officials who do not want to risk damage to the marine asset/personnel since repairs would be an undue cost. In the "no-go" situation, Vessel Assist will be called.

6.1.5 Implications

Safety is the overwhelming local driver of local maritime small vessel activity, but the potential threat posed by small suspicious vessels point to the need for improved Maritime Domain Awareness (MDA) in the Puget Sound region to enhance maritime security and safety in the

region. FSLTIPP maritime security players in the Puget Sound region have been able to improve awareness through information sharing and cooperation, but additional efforts could enhance further maritime domain awareness.

Joint patrols, where state and federal officials ride on sheriff's boats, have shown success – but those patrols are often limited to weekends and special events. Conducting additional patrols during weekdays or at random times, would provide additional timeframes where shared domain awareness is strengthened.

Another method of countering the potential threat from suspicious small vessels would be to provide a persistent sharable surveillance capability, such as SIGNALIS, which would allow detection, tracking, and classification of thousands of small vessels. Automatic classification of suspicious small vessels based on their operating profiles could allow law enforcement to respond more quickly to suspicious small vessels.

MDA in the Puget Sound region could also be improved by further increasing the responsible sharing of information already collected by FSLTIPP members of the security and safety community. Sharing current information feeds to authorized users on an enterprise architecture, such as the Integrated Maritime Domain Enterprise, would be another method of improving regional MDA using the community's existing sensors and activities.

6.2 Operational Planning and Scheduling – Use Case #2

6.2.1 Motivation

Planning and scheduling are critical activities performed on a daily basis by security and safety agencies and organizations across the FSLTIPP. The primary focus here is understanding the complexities of planning and scheduling for Puget Sound security and safety missions, and identifying opportunities to manage those complexities through an enhanced regional information sharing environment. Because a given mission can occur within a given agency (intra-) or across multiple agencies (inter-), this necessitates an investigation into both single and multiagency planning and scheduling processes.

While the USCG generally takes the lead on regional maritime interagency planning and scheduling, the majority of security and safety resources in the Puget Sound maritime area of responsibility are not federally controlled but rather are owned and operated by state, local, tribal, international, public and private entities. These resources could be leveraged to better achieve the Department of Homeland Security's mission to protect our maritime borders. Recent years have brought a growing focus at DHS on a "whole community" approach[103] to response and multi-agency collaboration.

Understanding how interagency collaboration can be achieved begins with understanding single-agency planning and scheduling processes and the barriers and opportunities to making single-agency plans transparent to other Port partners. In addition, for large organizations such as the USCG, even intra-agency planning and scheduling can have many interagency features, given the complex organizational structure and lines of authority. For these reasons, design concepts intended to enhance regional planning and scheduling systems and processes need to take both single-agency and multiagency operations into account.

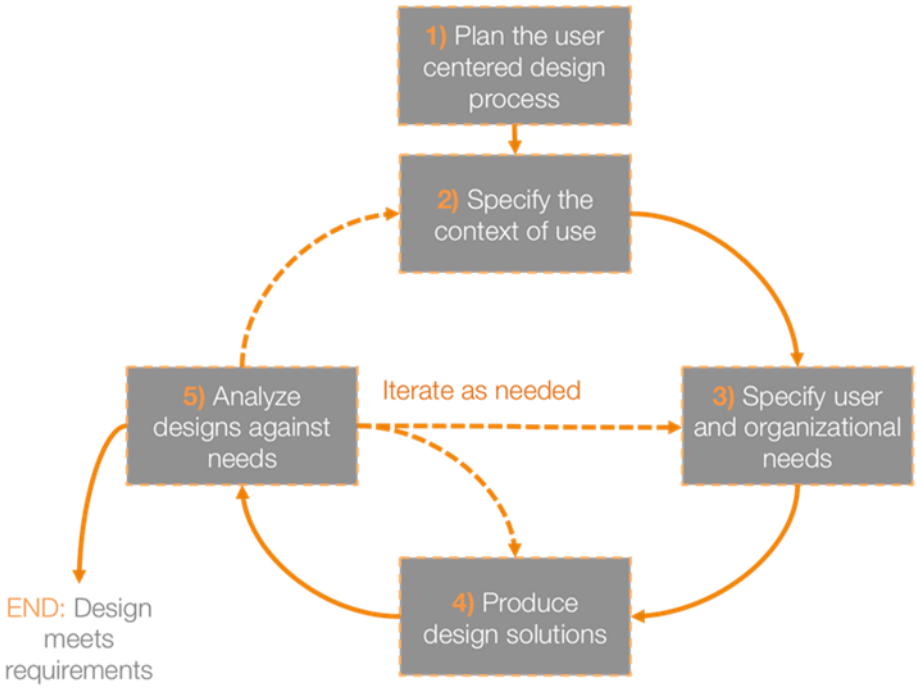
The SAFEPORT Act of 2006[104] established Interagency Operations Centers (IOCs) that include in their mission improved collaboration among FSLTIPP partners in planning and carrying out safety and security operations in key United States port regions. Planning and scheduling, along with shared maritime domain awareness, are important routes by which the IOC Program aims to improve multi-agency operations. There has been considerable effort to apply the potential of information technology (IT) to support these objectives. Towards this end, the IOC Program developed the *WatchKeeper* system (first deployed in 2010), which is intended to "improve tactical decision-making, situational awareness, operations monitoring and processing, and joint planning in a coordinated interagency environment. *WatchKeeper* provides a fully functioning and shared operational picture, shared mission tasking, and shared

[103] Federal Emergency Management Agency (FEMA). A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action." Ed., ed, 2011.
[104] "SAFE Port Act," in 103-347, ed, 2006.

response information to all users within the IOC, partner federal agencies, and local port partners."[105]

WatchKeeper provides a first step toward a regional planning and scheduling capability, but the full potential of technology to support this capability remains unrealized. One issue is that the usefulness of a collaborative planning tool is proportional to the number of agencies that actually use it, and although *WatchKeeper* has received positive reviews among federal operators (USCG, CBP), the majority of non-USCG port partners do not use the system.[106] The GAO found that one reason port partners do not use *WatchKeeper* is that its design focuses on the needs of Federal users. One of the main objectives of MOISA 2 was to demonstrate how a human centered approach to the design of Federal systems could incorporate the needs and perspectives of non-federal partners, as well as the benefits of doing this. Central to this approach is the articulation of a context of use (see *Figure 7*).

Figure 7: Human Centered Design Process (ISO 13407: ISO9241-210)



[105] "Privacy Impact Statement: United States Coast Guard, Interagency Operations Center (IOC) WatchKeeper," D. o. H. S. (DHS), Ed., ed, 2013.
[106] United States Government Accountability Office (GAO), "GAO-12-202: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers. ," 2012.

6.2.2 Objectives

This section articulates how federal and local port partners currently plan and schedule their resources in the context of regional mission accomplishment. Understanding these work processes is critical for many purposes, not the least of which is the use of this understanding in evidence-based, human-centered methods for the design of enhancements to these processes. The need to design human and work centered enhancements to the ISE is given impetus by the pending introduction by DHS S&T of a new planning and scheduling capability contained within the IMDE /CSS enterprise architecture.

In addition to (1) providing a better understanding of planning and scheduling work processes, and (2) helping us design enhancements to how this work is accomplished, this section, along with the following Section 7, addresses a third need – the need for a repeatable process to incorporate port partners' input into the design of future systems to support interagency operations. As a pair, Sections 6.2 and 7 go a long way towards meeting the GAO recommendation that, *"the Commandant of the Coast Guard should direct the IOC Project Manager to develop, document, and implement a process to obtain and incorporate port-partner input into the development of future WatchKeeper requirements."*[107] The process, demonstrated here in collaboration with IMDE/CSS developer SRI International, is an application of the iterative Human Centered Design methodology—which begins with the specification of the context of use (*Figure 7*).

Thus, this chapter and the following chapter describe and demonstrate a repeatable methodology for incorporating community input into the design of information sharing technology and processes. Through this work, we seek to understand and positively influence how the pending delivery of a new planning and scheduling capability contained in the IMDE/CSS enterprise architecture might impact community members' work and present opportunities to enhance these processes.

[107] United States Government Accountability Office (GAO), "GAO-12-202: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers. ," 2012.

6.2.3 Methods

To articulate a planning and scheduling use case that encompassed both single-agency and inter-agency operations, MOISA researchers conducted in-person and phone interviews with members of the Puget Sound safety and security community. The interviews focused on participants day-to-day planning and scheduling activities and the information they rely on in the service of these activities. A copy of the semi-structured interview protocol can be found in Appendix C:. Interviews were documented in field notes and, in one case, an audio recording. The researchers also examined information artifacts (such as examples of agency schedules and plans) that interviewees provided.

6.2.4 Participants

A subject matter expert identified relevant stakeholders at the following agencies who participated in interviews and observational sessions: King County Sheriff's Office Marine Unit, Port of Everett Security, Skagit County Sheriff's Office, Jefferson County Fire and Rescue, Drug Enforcement Agency, and USCG Enforcement Division at Sector Puget Sound. This initial sample was selected to provide a useful mix of Federal and non-federal perspectives, but it by no means covered our entire diverse security and safety community.

6.2.5 Results

In this section we describe the current state of planning and scheduling for our interviewees and how this aided us in scoping the use case in support of the human-centered, iterative design and development cycles described in the following chapter. Our analysis provided insights into factors that will impact the design of planning and scheduling business processes and system enhancements. We found that current planning and scheduling processes require planners to spend considerable time and effort manually integrating information from a variety of information resources; that agencies have limited visibility into one another's current operations and even less into their future plans; that the specificity of plan and schedule documentation varies by agency and mission type (interagency vs. single agency); that agencies

have different concepts of planning and scheduling tasks and resources; and that common core information attributes transcend the boundary between pre-planned and emergent events. We conclude this section with an explanation as to how these findings guided us in articulating the case used in the collaborative design and development activity with SRI international described in the following chapter.

6.2.5.1 Current processes require manual integration of information from multiple resources

Current planning and scheduling processes require planners to manually integrate information from a variety of information resources. Table **5** is an inventory of the different information resources participating agencies use in their current planning and scheduling processes for our interviewees. Some of these are electronic or enterprise systems that facilitate sharing, but many others are either paper-based or in a format that is difficult to share (i.e., a staff schedule written on a whiteboard).

Some of the computer-based systems require significant manual work in order to adequately support current planning and scheduling needs. For example, Jefferson County Fire is primarily a response organization, and their plans are encoded into a CAD system that uses computer algorithms to dispatch resources. Although this system is intended to offload decision-making from human operators, it ends up adding significant overhead; Jefferson County Fire personnel spend about two hours twice a week manually modifying the algorithms in order to ensure that they reflect the current staffing and resource availability. The knowledge of how to modify these algorithms is fairly specialized and only one person at the agency currently has the skills to make these modifications.

Another example is the classified MHS-OPS system used by the Navy and the Coast Guard. Coast Guard Planners need information from this system at their desks as they are constructing their plans, yet the computer that houses the system is on a different floor from the planners' work area. To get around this, planners transcribe information from the classified system into handwritten notes that they then carry back to their desks.

The problem of manual integration is magnified in the case of interagency operations. Our interviewees reported using FEMA Incident Action Plan (IAP) forms to plan interagency operations, which are often filled out on paper and then scanned and transmitted via email, where recipients often need to print and share in hardcopy again. This manual work is in addition to the manual integration agencies are already doing to maintain their own intra-agency plans. The task of manually integrating information resources for interagency operations plans is particularly onerous for the USCG Sector Enforcement Division whose job it is to combine IAP pieces into a single cohesive plan and then distribute this to other agencies participating in the operation. As is shown in Chapter 7, this division alone would eliminate numerous time-consuming unproductive overhead tasks through the use of an appropriate designed, more transparent system.

Table 5: *Information resources used by interviewees in current planning and scheduling* processes.	
Agency	**Information Resources**
County Fire	• New World Systems CAD • Blue Force Tracking • Eyes on scene • Cell phone • Radio (Channel: marine 22 alpha) • Excel schedule
DEA	• Phone • Western State Information Network (WSIN) – by phone • High Intensity Drug Trafficking Area (HIDTA) – by phone
Skagit County Sheriff's Department	• Excel schedule • Email • InTime ISE Scheduling software • Spillman Mobile AVL Mapping • Radio • Cell phone
USCG	• MHS-OPS • Hand written notes transcribing info from classified system • CGMS • ALMIS • AOPS • Outlook Calendar • Staff schedule on whiteboard • Phone • Email • Blue Force Tracking (WatchKeeper)
King County Sheriff's Department	• Staff schedule on whiteboard • Cell phone text messages • Radio • Email
Port of Everett Security	• Cell phone • Cargo manifest • Ship's schedule • Operations schedule • In-person joint planning meetings • HSIN notes delivered via email • Fusion Center bulletins • Email

6.2.5.2 Limited visibility into others' current missions

Interviewees reported having little visibility into the availability and location of partners' resources in real time. Having this visibility is so important for some agencies that they rely on labor-intensive workarounds. For example, Jefferson County Fire has designated highpoints in their area where they can send a staff member with binoculars to view the vessels that are out on the water and report back to headquarters via radio.

The value of visibility into the status of partner activities can vary depending on the agency and the type of information. For example, King County Sheriff's Marine Unit has access to Blue Force tracking that could be used to see other nearby resources on the water, but according to our interviewee, it is rarely used. One reason for this is that only one of their boats has the necessary equipment to view the Blue Force tracking data, but the interviewee did not feel that the benefit of retrofitting the other boats to have this capability would outweigh the cost because "it is a technology that is just not really used." They do not base their patrol decisions on the location of other agencies' resources, and when they need support from other agencies to handle emergent issues, their current practice is to put out a call to all nearby resources rather than request support from a specific resource based on its proximity to the event.

On the other hand, many interviewees specifically identified the location of partner resources as something they were eager to have, but some were not aware of existing tools and their availability. For example, the DEA, which does not control any marine assets, would like to see what marine resources are on the water that might aid them in maintaining surveillance, but when asked whether he uses Blue Force Tracking, our DEA interviewee did not know how this could be made available to him.

6.2.5.3 Information on agency schedules is siloed

Interviewees did not report sharing their day-to-day plans and schedules outside of planning interagency operations. Some interviewees see no need to share this information beyond the existing informal lines of communication (See MOISA 1 report). King County Sheriff's Department Marine Unit, for example, stated that because of their close geographic proximity to

neighboring LLE (Mercer Island PD, Seattle PD), they are typically aware of what one another are doing day-to-day, despite the fact that their plans are not explicitly shared. One interviewee likened it to working in an office with cubicles and knowing if and when the person in the cube next to you shows up to work.

For LLE interviewees, knowing where partnering LLE agencies plan to patrol does not impact their own decision-making on where their own resources will patrol because jurisdictional boundaries are clearly defined—LLE officers will patrol their own AOR regardless of whether a neighboring LLE resource also appears to be covering the same area. However, there were some cases in which having visibility into federal agency plans would impact interviewees' decision-making regarding their own plans, to the end of avoiding overlapping federal coverage and overlapping federal and local coverage of an area. For example, if USCG Station Bellingham had visibility into CBP's patrol schedule, they would adjust their own patrol schedule to avoid overlapping coverage. Similarly, if King County Sheriff Marine Unit had visibility into the planned location of USCG resources in their AOR, they would adjust their own patrol schedule to more evenly distribute resources throughout their AOR.

There is a general perception among local law enforcement interviewees that other port partners do not need to know information regarding their future plans for day-to-day operations.

6.2.5.4 Varying natures and levels of specificity in plans and schedules

Different agencies have different notions of what constitutes a plan (see Section 6.2.5.5 below) and they include different levels of specificity in their plans and schedules. There is also a marked difference in the nature and specificity of single agency vs. interagency plans.

For interviewees, day-to-day plans often have important improvisational elements. Most LLE and USCG stations do not specify patrol locations beyond a very general description of the waterway and they often do not specify patrol start and end times, even for patrols planned well in advance. The decision of the patrol route and when to start and end a patrol on a given day is left up to the individual operator who may base this decision on historical patterns (e.g., they may decide to patrol areas that have a history of high seasonal traffic), the

current conditions (i.e., they may decide to stay in calm waters where there are likely to be more recreational boaters), or even on a whim. Maintaining this flexibility and adaptability in day-to-day plans is important to their successful execution as conditions that impact resource allocation are constantly shifting—weather, the availability of staff, and the rise of emergent incidents to which they must respond.

Part of the reason for this range of specificity is that some plans are created to address problems that are clearly defined (e.g., how can we safely move a particular oil drilling rig through a specific high-traffic waterway within a certain timeframe) while other plans are created to address problems that are far less specified, or may not even be conceptualized as "problems" at all. Many daily operations are not triggered by situational information, for example, USCG escorts of ferries, cruise ships and commercial vessels are generally determined by a formula that establishes a quota of activity based on number of ferries, number of commercial vessels, etc.

6.2.5.5 Differences in the Conceptualization of Planning and Scheduling Tasks and Resources

The primary planning and scheduling task for LLE and USCG Stations on a day-to-day basis is to assign crew and staff to vessels and missions. In contrast, the primary planning and scheduling task for USCG Sector Enforcement is to collect plans from stations and other agencies and integrate them into *Execute Orders* that include information at the level of vessel location and mission, but not crew and staffing. This brings a challenge to the design of a single solution that meets the planning and scheduling needs of all partners. At the heart of this challenge is the fact that individuals in different roles think about resources in different ways—for some, resources are primarily boats; for others, particularly in LLE, resources are primarily people and/or equipment. A collaborative planning and scheduling tool will need to support the scheduling of this variety of resource types.

Existing planning and scheduling tools such as *Watchkeeper* include boat specifications in vessel inventory information. This supports planners in considering the boat's capabilities (e.g., speed) and limitations (e.g., fatigue limits) before determining that it is the appropriate resource

for a given mission. Similarly, planners consider the "specs" of people and equipment resources. Not all personnel resources have the same qualifications, and equipment resources sometimes require operators with specific skills to use them (e.g. rad/nuc training, diving skills). Just as they do in scheduling boats to missions, planners determine which personnel and equipment they should use not only on the resources *availability*, but also on a particular resource's or combination of resources' *capability* to meet mission needs.

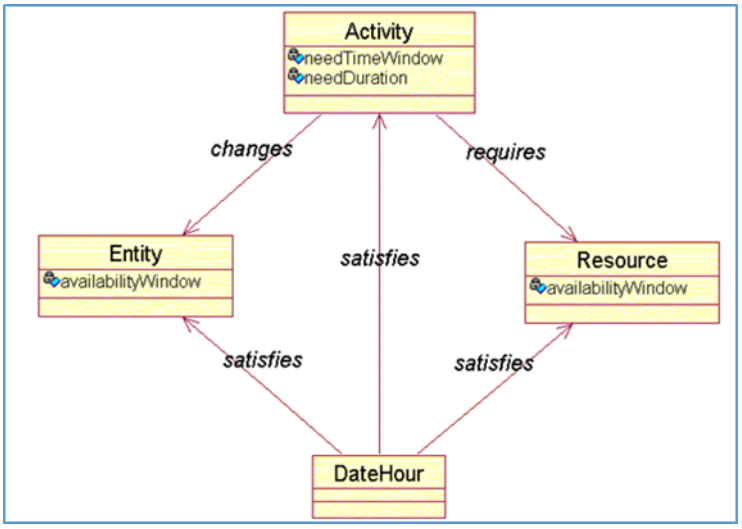
The processes for actually scheduling these different types of resources are also different. For example, personnel resource needs to be made aware of a schedule change, whereas a piece of equipment does not.

6.2.5.6 Core concepts that cuts across planning for scheduled vs. emergent events

While our interviews uncovered a wide range of differences across regional planning and scheduling activities, they also revealed common underlying principles that can be used to integrate design across these differences. Of particular relevance to this use case are the differences that arise between pre-planned and emergent planning. Rather than representing irreconcilable strategies, these differences can be viewed as existing at different points along a single continuum from long-range plans to what is happening right now. As depicted in *Figure 8* this type of integration stems from a common underlying concept of planning and scheduling that cuts across agencies, missions and time horizons.

The template provided by *Figure 8* allows us to analyze how different forms of planning that appear very different on the surface actually follow a core concept (a.k.a. *ontology*) underneath. Table **6** illustrates the core concept by comparing examples of information attribute values in planning for events that are scheduled versus events that are emergent. The values of the attributes in rows three and four are what really sets apart a pre-planned versus emergent event.

Figure 8: Ontology of Planning and Scheduling



Both activities require the same types of information: What is the entity, where is it and in what condition, what is the activity that needs to be performed on the entity, what resources are needed, and when can they be brought to bear on the activity? What distinguishes the information in a preplanned vs. emergent scenario is the value of the information attribute.

Table 6: *Information attributes for planning and scheduling and comparison of example values in scheduled vs. emergent events*

Information attributes	**Scheduled event**	**Emergent event**
1. What is the entity and its situation?	An important foreign dignitary is visiting the area	Overturned vessel
2. What is the needed activity?	Maintain security around the visitor	Rescue passenger
3. Where will the entity be at the time of the activity?	Transit route, including start and end points and stops	Real-time location of vessel available via AIS
4. When should the activity take place?	Two years from now	Now
5. Which resources should be used to carry out the activity?	USCG vessel 1, USCG vessel 2	Whichever can get there fastest

During both planned and emergent events, planners are making risk-based decisions regarding whether and how to allocate their resources in support of the activity. Decision-making for emergent events is constrained and somewhat simplified by the urgency with which the response is needed, but in the case of pre-planning, factors such as economics and competition come into play. This becomes even more complicated for pre-planning of interagency operations in which agencies often need to share their own operations schedules. This is supported by our prior research during MOISA 1 that found that for non-emergent operations, "issues of ownership, competition, economic impact, and the sustainability of operations effect information sharing."[108]

The two events in Table **6** illustrate the breadth of the time horizon for planning, and this range of time horizon accounts for many differences in planning. For events that are scheduled, the farther out the event the more planners try to optimize the utilization of resources to get the best use of them for the cost. In contrast, emergent events that threaten human lives require immediate action, so cost factors are subordinated. For longer term emergency planning, resources can be configured and positioned based on some optimized combination of response time to anticipated need locations and cost of stationing them in those areas.

6.2.5.7 Articulating a Design "test case" from the general use case

Based on our understanding of the planning and use case, we articulated a design "test case" to drive our collaborative design and development activities with SRI and the regional community (see Section 7). Our criteria for selecting valid test cases was based on our analysis of the information used in the service of planning and scheduling tasks, gaps and inconsistencies in information flow, and pain points in the agencies' current processes. Some pain points were distinct to single agencies, but one problem that was consistently brought up in all interviews

[108] M. Haselkorn, M. Zachry, K. A. Butler, M. O. Braxton, M. Rowell, and D. Dailey, "Maritime Operational Information Sharing Anslysis, Final Report (Year 1)," University of Washington, Department of Human Centered Design & Engineering, National Maritime Intelligence-Integration Office (NMIO), Program Manager for the Information Sharing Environment (PM-ISE), Department of Homeland Security (DHS) Interagency Operations Center2014.

was the challenge of achieving transparency of information for interagency operations. Such plans require coordination and information sharing among all agencies involved in the operation. We selected advanced planning of interagency operations for our test case because it was frequently mentioned as a pain point that was not specific to any one agency and was relevant to all users. USCG Enforcement provided us with an example of an interagency operations plan (IOP) for a relatively common occurrence in the Puget Sound: the movement of an offshore drilling unit from a Port in Puget Sound toward Alaska. This test case and testing activity are further described in the following chapter.

6.2.6 Discussion

We articulated a variety of community perspectives on planning and scheduling and found several "pain points" associated with single-agency and interagency planning and scheduling that point to the desirability of an improved system and process: planners currently get the information they need from a variety of sources that are not currently well integrated (requires manual integration) and in some cases they don't have the information they need at all (little visibility into current operations; plan information is siloed). A "keystroke neutral" solution that provides transparency of relevant information to planners will reduce planners' workloads, the risk of errors and redundancy, and increase efficiency and mission effectiveness.

Designing systems to support planning and work processes of varying levels of specificity is a known problem in the field of Computer Supported Cooperative Work (CSCW). Concepts of the role of plans in work come from two distinct schools of thought: (a) the workflow tradition in which a plan is a part of an organized process by which actors analyze a problem and a set of solutions before choosing and then executing a solution. This view supports the development of defined organizational processes. The second tradition is (b) situated action in which a plan is not executed, but is rather a resource to be used in action (a jumping off point or "going in" position). This view supports the use of flexible communication support systems that allow actors to nimbly adapt to changing circumstances. Both of these concepts come with limitations. The procedural models advocated by (a) have the potential to take away actors necessary flexibility, and more flexible solutions advocated by (b) can lack

adequate decision support. A solution that supports the broad range of agency activity including prescribed and ad hoc processes is needed.[109]

Another key principle is that in order for a planning and scheduling tool to be useful for interagency operations, its data sources need to be kept current by partnering agencies for their day-to-day plans. Our findings that different agencies have different ways of conceptualizing resources and planning and scheduling tasks, and that they currently document their plans with varying levels of specificity, have implications for the design of a system that will support planners in both day-to-day, single-agency plans and interagency operations planning.
A system to aid in single-agency planning day-to-day should support planners' decision-making regarding their resources' capabilities as well as availability. Because capability is often a combination of resources (e.g., a piece of equipment and a person who is trained to operate it), planners need to have information on personnel and equipment integrated with information on vessel schedules.

Articulating the ontology of planning and scheduling is a prerequisite for data integration. The finding that planning for events that are both emergent and planned in advance rely on common information types suggests that a single tool or process could be designed to support planning activities anywhere along the continuum of pre-planned to emergent events.[110] The ontological relationships between planning and scheduling concepts presented in this analysis are consistent with prior work that articulated an ontology model for planning and scheduling aircraft maintenance.[111]

The following Section 7 takes this analysis of the planning and scheduling use case and applies it to a specific design and development challenge.

---

[109] A. Bernstein, "How can cooperative work tools support dynamic group process? bridging the specificity frontier," in Proceedings of the 2000 ACM conference on Computer supported cooperative work, 2000, pp. 279-288.
[110] Y. Weihong, "Research on Maritime Search and Rescue Decision-Making Ontology Model," in Environmental Science and Information Application Technology, 2009. ESIAT 2009. International Conference on, 2009, pp. 140-142.
[111] K. A. Butler, J. Zhang, C. Esposito, A. Bahrami, R. Hebron, and D. Kieras, "Work-Centered Design: A Case Study of a Mixed-Initiative Scheduler," CHI -CONFERENCE-, vol. 1, pp. 747-756, 2007.

7 MOISA's Role in IMDE Development

During MOISA 2, we established a design and development collaboration among the University of Washington's (UW) Department of Human Centered Design & Engineering (HCDE), IMDE/CSS developer SRI International (SRI), and key members of the Puget Sound security and safety community. This collaboration in support of design, development, and demonstration of a planning and scheduling module of IMDE/CSS provided a practical opportunity to demonstrate how research conducted under MOISA 1 and 2 can be applied to improve and enhance information technology (IT) innovation in systems for regional security and safety. Specifically, this collaboration demonstrated a design and development methodology that:

- Integrates port-partner input into the design and development of systems.
- Embeds design, development and fielding in the context of a deep understanding of the existing information sharing environment.
- Facilitates transition, adoption, and sustainment by incorporating end users in design decisions
- Provides agility and flexible response to user input through rapid, iterative design-build-evaluate cycles
- Provides formative evidence for design decisions based on mission enhancement.

The requirement that IT deliver predictable, measurable benefits, particularly in health- and safety-critical domains, has never been more essential. Particularly in government and service systems, human- and user-centered design (often used interchangeably but evolving towards "human centered") are increasingly being recognized as part of a much-needed shift in our approach to IT development. MOISA 2 culminated with the establishment of a design and development team in support of the IMDE/CS project, the application of our study of the planning and scheduling use case to the work of this team, and the completion of two iterations of a design-build-evaluate cycle that demonstrate a state-of-the-art technology innovation methodology for the design, development, and transition of maritime security systems.

7.1 Background: Technology Innovation in Government

While MOISA is making considerable strides in advancing evidence-based human centered design in the maritime safety and security arena, the demand for evidence-based IT has been most public in the Healthcare sector, stimulated by recent studies[112] and reports[113, 114, 115] that revealed that in some cases, government-stimulated IT initiatives have even caused damages rather than improvement. To address this problem, the US Department of Health and Human Services (DHHS) established CFR Part 170, RIN 0991-AB82. Under the HI-TECH act, this legislation is part of the Stage 2 meaningful use (MU) criteria that mandates changes to the way that Health Information Technology (HIT) has traditionally been designed—since 2014, HIT vendors must demonstrate that their products are designed via "user-centered design" (UCD) methods.[116] This first articulation of UCD into law has led to expanded attention to this methodology throughout the federal government and industry.

In 2013, the US Government created the United States Digital Service (USDS), with the mission to "transform how the federal government works for the American people" through changing the way we design citizens' interaction with Web-based services. [117, 118] In one example, 18F is a USDS project dedicated to changing the way the government designs Web services and procures IT. According to 18F's former Executive Director, Greg Godbout, "the number one biggest problem that government should be addressing right now is user-centered design

---

[112] Kellermann, A.L. and S.S. Jones, What it will take to achieve the as-yet-unfulfilled promises of health information technology. Health affairs, 2013. **32**(1): p. 63-8.
[113] Abelson, R. and J. Creswell, In Second Look, Few Savings From Digital Health Records, in New York Times. 2013.
[114] Abelson, R., J. Creswell, and G. Palmer Medicare Bills Rise as Records Turn Electronic. The New York Times, 2012.
[115] Abelson, R. and J. Creswell, Report Finds More Flaws in Digitizing Patient Files, in New York Times. 2014: New York, NY.
[116] DEPARTMENT OF HEALTH AND HUMAN SERVICES Office of the Secretary, 45 CFR Part 170, RIN 0991-AB82, Health Information Technology: Standards, Implementation Specifications, and Certification Criteria., D.O.H.A.H. SERVICES, Editor. 2012. p. 54186 – 54189.
[117] *18F*. January 27, 2015]; Available from: https://18f.gsa.gov/.
[118] *United States Digital Services*. January 27, 2015]; Available from: http://www.whitehouse.gov/digital/united-states-digital-service/story.

versus (what he calls) stakeholder-centered design[119]." He recalled thinking that "in almost none of these (federal government) projects do they talk to an actual end user.'"[120] Godbout says that user-centered design is "really very revolutionary inside the federal government and causes a lot of pain as we insist that people work this way."[121]

USDS recognizes that government websites and other IT efforts constrain and enable the flow of information that is critical to the delivery of government services. As seen in the troubled rollout of the healthcare.gov Website, the design of IT impacts the flow of information in a service system, and we are in effect designing the workflow by which that service can be delivered.

The results of the IMDE/CSS design activity that we present here constitute a cutting edge example of the growing trend toward human centered design in both industry and government. In the following section we describe the Human Centered Design methodology and how it works to ensure that IT adds value.

7.2 Human Centered Design Methodology

Human centered design is a principled approach to iterative design and development with the user community on the team. The principles of this approach are part of a national standard described in ISO 9241-210, Human-centered design for interactive systems.[122] These principles are:

- The design is based upon an explicit understanding of users, tasks and environments.
- Users are involved throughout design and development.

---

[119] In this case, "stakeholder" denotes government agencies with interests distinct from those of individual users.

[120] Naylor, B., Remaking The U.S. Government's Online Image, One Website At A Time, in National Public Radio: All Tech Considered. 2015, National Public Radio.

[121] International Organization for Standardization (ISO), ISO FDIS 9241-210. Ergonomics of human system interaction - Part 210: Human-centred design for interactive systems (formerly known as 13407). 2010 Switzerland.

[122] International Organization for Standardization (ISO), ISO FDIS 9241-210. Ergonomics of human system interaction - Part 210: Human-centred design for interactive systems (formerly known as 13407). 2010 Switzerland.

- The design is driven and refined by user-centered evaluation.
- The process is iterative.
- The design addresses the whole user experience.
- The design team includes multidisciplinary skills and perspectives.

Figure 9, which was introduced in the previous Section 6.2, describes the iterative human centered design process, largely captured in ISO 13407 and ISO 9241-210. Multidisciplinary design teams cycle through steps 2-5 to design, build, and evaluate design concepts with the user community. Each design iteration comprises these steps. Through this HCD process, designers not only put users at the center—we actually bring them onto the design team and co-design with them.

Figure 9: Human Centered Design Process (ISO 13407: ISO9241-210)

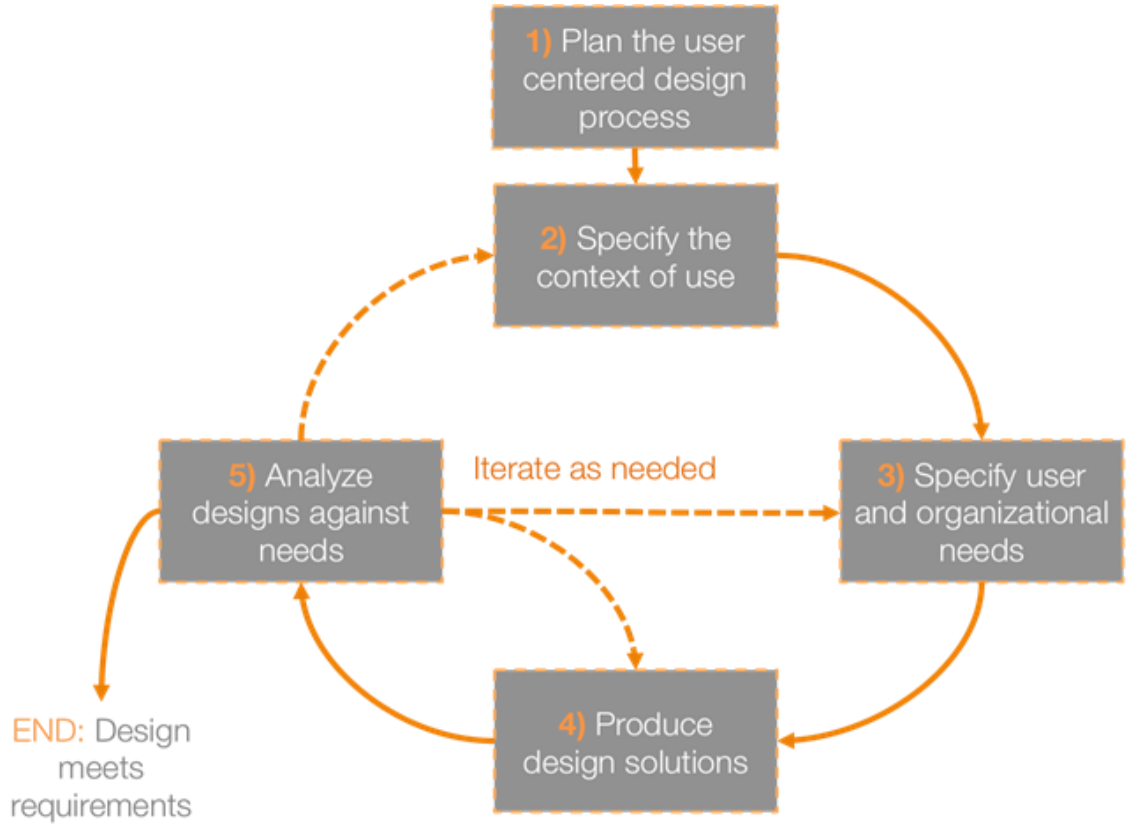
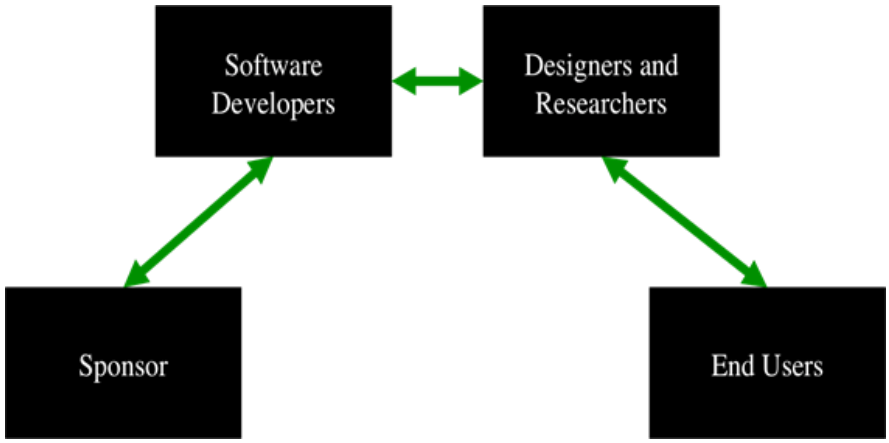


Figure 10 shows the roles and relationships in an HCDE process. This close collaboration between the design team and developers reduces the gap between project sponsors and end users. The result is better design, faster and with less cost, less waste, and less risk. Using this approach, grounded in a close partnership among the user community, designers, and developers, we can:

- Base design decisions on evidence
- Co-design with a complex set of stakeholders with differing missions, jurisdictions, practices, policies, funding sources, systems, cultures, etc.
- Increase the ownership of the design by the user community
- Integrate transition issues into design and development

Figure 10: Roles and Relationships Among System Stakeholders



7.2.1 Standards for Usability Testing

A number of standards have evolved in support of human- and user- centered design. ISO 9241-210 lays out the principles of HCD, but does not provide specifics with exactly how HCD activities are to be evaluated. In 2003 a team led by NIST developed a standard for reporting usability test results for software products that was quickly adopted by ANSII and shortly afterward as ISO Standard 25062. The standard, now called The Common Industry Format (CIF) was the codification of best practice in industry. The test cases are structured to

focus on those system features that are intended to add value to operations or business. The CIF requires measures that include:

- Task completion success rates,
- The time required for each task if it is completed,
- Errors, and patterns of errors, and
- User satisfaction.

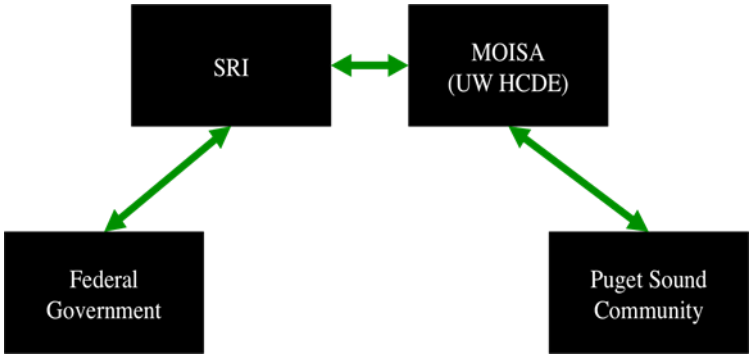
These measures establish an objective connection between a new software system and its impact on the operations it is supposed to improve. If needed, a test can also be conducted on existing systems to establish a baseline for comparison. The CIF report also describes the qualifications of the test users, the training they received, and enough about the conditions of the test to allow the test to be replicated.[123] The MOISA team used these standards to plan the test reported in the remainder of this chapter.

7.3 The MOISA-SRI Collaboration to Introduce HCD into the DHS-S&T IMDE/CSS Project

Under MOISA, UW worked with SRI to engage the regional operational community in the design, development, and transition of the Integrated Maritime Domain Awareness/Coastal Surveillance System (IMDE/CSS), a DHS S&T Borders and Maritime Security Initiative introduced in Section 5. SRI International is a non-profit research and development organization that is contracted by DHS to develop the IMDE/CSS. *Figure 11* shows the roles and relationships among DHS Sponsors, SRI developers, UW researchers and designers, and the user community.

[123] Usability.gov. *The What and Why of Usability: Reporting Usability Test Results*. 2015; Available from: http://www.usability.gov/how-to-and-tools/methods/reporting-usability-test-results.html.

Figure 11: Roles and Relationships Among Stakeholders
in the DHS-S&T IMDE/CSS Design Activity



Current IMDE/CSS plans include the demonstration of capabilities that will support information sharing among users doing both inter- and intra-agency planning and scheduling in the case of both day-to-day and emergent events. For the purpose of this report, planning refers to the process by which users analyze operational objectives, required activities, and desired outcomes to articulate how resources and capabilities need to be used in order to complete the operation; scheduling refers to the advance assignment of resources to operations. SRI developed an initial design concept and a front-end prototype of a planning and execution suite of widgets to deliver these planning and scheduling capabilities. In June 2015 SRI began working with UW to mature this concept, beginning with the application of our analysis of a planning and scheduling use case (described in Section.6.2), and continuing through iterative design-build-evaluate cycles as described below.

7.3.1 METHODS

The team of software developers (SRI), researchers and human-centered designers (UW) collaborated with project sponsors and members of the user community to embark on two design-build-evaluate iterations on the design of the IMDE/CSS planning and scheduling capabilities. This design activity was conducted in the field with operational users.

7.3.1.1 Iteration 1

MOISA researchers conducted in-person and phone interviews with five diverse but representative users to articulate a Planning and Scheduling use case for the purpose of exercising the current prototype of a IMDE/CSS module. The schedule called for delivery as part of an Operational Demonstration scheduled to take place in Puget Sound in March 2016. The full results of these interviews are summarized in Section 6.2. Table **7** is a summary of the interviewees and their engagement with the iterative prototyping team in iterations 1 and 2.[124]

Table 7: *Summary of test participants, interviews and test sessions*

Agency type	Organization	Iteration 1 Interview	Iteration 2 Test Session
Federal Law Enforcement	Drug Enforcement Agency - Seattle	6/23/15	---
Federal Law Enforcement	USCG Sector Puget Sound Enforcement	6/24/15 (+ 3 follow ups)	8/13/15
Federal	USCG Station Seattle	---	8/13/15
Federal	USCG Station Bellingham	---	8/14/15
Local Law Enforcement	Skagit County Sheriff	6/25/15	8/11/15
Port Security Manager	Port of Everett Security Manager (Head of the AMSC technical subcommittee)	6/26/15	8/14/15
Fire Department	East Jefferson Fire & Rescue	6/22/15	---

From these interviews, we learned key workflow information such as that for some users, staffing information is critical to their planning decision making, while for other users, creating maps of where resources are planned to be at the start of an operation is an important task that currently requires a significant amount of manual integration. Based on findings such as these, the software developers added capabilities to assign staff to boats and create mission maps for planning purposes. Users then validated these design concepts as a part of iteration 2 testing described below.

[124] For the purpose of usability evaluation, five users is optimal. Studies have shown that the best result come from testing no more than five users. *Nielsen, Jakob, and Landauer, Thomas K.: "A mathematical model of the finding of usability problems," Proceedings of ACM INTERCHI'93 Conference (Amsterdam, The Netherlands, 24-29 April 1993), pp. 206-213.*

7.3.1.2 Iteration 2

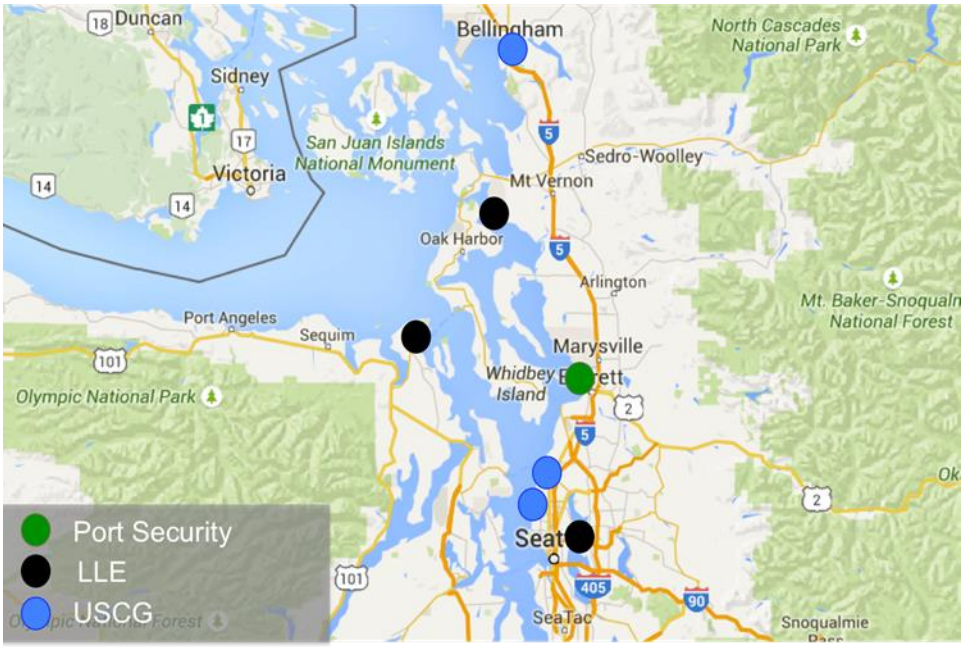
The MOISA iterative prototyping team conducted an onsite usability evaluation using a Web-based demonstration version of the IMDE/CSS planning and scheduling module. The demonstration version of the module includes several widgets designed to support different aspects of planning and scheduling tasks. Table **8** lists the different widgets under evaluation and a brief description of the key functions available in the demo on which the evaluation focused.

Table 8: *List of key functions in IMDE/CSS planning and scheduling widgets exercised in iteration 2*

Widget	**Key functions**
Calendar and scheduling	• Display regional agencies' resources and resource availability on a day's schedule • Provide access to individual resource specifications, point of contact, and staff scheduling • Display scheduled missions and mission duration on a day's schedule • Provide access to the details of individual missions • Allow users to assign available resources to scheduled missions
Communication	• Provide users with a searchable directory of other users across the region • Allow users to communicate with one another via live chat
Mission planning	• Provide a template for organizing and sharing mission planning information (e.g., point of contact, mission risk, resources assigned, etc.)
Map	• Represent mission location on the map • Represent resource location on the map • Provide limited information on missions and resources that appear on the map • Allow users to manipulate planned location of resources and missions on the map

A MOISA subject matter expert identified potential users in the Puget Sound maritime community and assisted the iterative prototyping team in recruiting these users via email. The five users represented a broad geographical area (*Figure 12*) and a range of agencies from port security, local law enforcement and federal, USCG law enforcement at the sector and station levels (Table **7**).

Figure 12: Map of participants' geographic location



Based on the general use case, UW developed a test protocol around a specific test case involving the secure escort of an oilrig platform being towed towards Alaska. A copy of the test documentation including this protocol can be found in Appendix D:. A MOISA researcher followed this protocol to conduct one-on-one test sessions with the five representative users. Users interacted with the prototype at their own workstations using a test computer provided by the research team. Test sessions were screen and audio recorded using Apple's QuickTime Player Application, and recordings were stored locally on the test computer. The test administrator and data logger sat alongside the users as they conducted the test. During the test session, the test administrator provided users with a brief over-the-shoulder training on how to use the features of the software demo that were relevant to the test case. Following the training, users were guided through the planning and scheduling test case and prompted to complete the case a second time without guidance. Users were then asked a series of quantitative and open-ended questions about their experience. A copy of the test documentation including the questionnaires is included in Appendix D:. Each test session lasted approximately one hour. The sessions captured each participant's navigational choices

using the software demo, task completion rates, comments, overall satisfaction ratings, questions and feedback.

Participants ran through the Planning and Scheduling test case using a software demo that was pre-populated with simulated schedule data derived from example schedules collected during field research. Participants attempted to complete the following tasks:

1. Review their agency's resource schedule for the current day
2. Familiarize themselves with the plan and schedule for an interagency operation scheduled for a future date
3. Decide whether and how their own agency's resources might be allocated in support of the operation in 2.
4. Schedule any resources they wish to allocate in support of this mission, including assignment of the desired starting location for the mission.

Post-test, participants completed a System Usability Scale (SUS). The SUS is a well-validated instrument for obtaining a single numeric score to indicate users' subjective assessment of system usability.[125, 126]

Additional subjective measures included participants' overall satisfaction with the design concept presented by the demo, their behavioral intent to use such a design, and their feelings on trust, privacy, and information sharing and safeguarding associated with the design concept. For these structured questions, participants were asked to rate their agreement with statements on a Likert scale of 1-5 (1 = strongly disagree; 5 = strongly agree). The open-ended questions focused on what participants liked or found difficult about using the demo and what they might change about this current version.

7.3.2 Results

The following results include a summary of quantitative results from questionnaires as well as a summary of issues abstracted from qualitative video data and open-ended survey

[125] Bangor, A., P.T. Kortum, and J.T. Miller, An empirical evaluation of the system usability scale. Intl. Journal of Human–Computer Interaction, 2008. 24(6): p. 574-594.

[126] Brooke, J., SUS-A quick and dirty usability scale. Usability evaluation in industry, 1996. 189(194): p. 4-7.

questions. The research team is continuing to analyze quantitative data on task completion rates, time on task, the results of which will be included in a separate report that will be delivered to the software developer, SRI International.

7.3.2.1 Quantitative results

Participants placed the IMDE/CSS demonstration in the 78th percentile of the System Usability Scale (SUS) with scores ranging from 70-85. SUS Scores can range from 0-100 with higher scores indicating better system usability. The SUS is not meant to be an absolute measure of usability but is rather most useful in comparative analyses of candidate designs. Initial SUS scores can be used as a baseline against which we evaluate future iterations. Yet we can still attach some meaning to the mean SUS score — in their comprehensive evaluation of the SUS in use, Bangor, Kotrum, and Miller found that "products which are at least passable have SUS scores above 70, with better products scoring in the high 70s to upper 80s."[127] The IMDE/CSS demo's mean SUS score of 78 suggests that the design concepts have room for improvement, but they are headed in the right direction.

The following list summarizes the quantitative results from the additional questionnaire. These results are also summarized in a table that appears at the end of this chapter (Table **10**):

- All of the participants (5/5) agreed (i.e., agree or strongly agree) that a system like this would be helpful for their agency and agency partners if it were available.
- All of the participants (5/5) would recommend a system like this to a friend or colleague.
- The majority of participants (4/5) reported being satisfied with this version of the system.
- The majority of participants (4/5) reported that a system like this would contribute to their agency's ability to collaborate with partner agencies for improved mission accomplishment.
- The majority of participants (4/5) agreed that if they had a system like this at work, they would use it.

[127] Bangor, A., P.T. Kortum, and J.T. Miller, *An empirical evaluation of the system usability scale.* Intl. Journal of Human–Computer Interaction, 2008. **24**(6): p. 574-594.

- Just over half of participants (3/5) felt that they need to have a system like this
- Just over half of participants (3/5) felt that this version of the system worked the way they wanted it to work.
- Just over half of participants (3/5) believe that partner agencies will be satisfied with a system like this.
- Just over half of the participants (3/5) felt unable to answer whether a system like this would be trustworthy.
- Although the majority of participants (4/5) felt that partnering agencies would have concerns about security, privacy, and confidentiality associated with a system like this, all of the participants (5/5) felt that the test case did not provide them with enough information to answer whether this version of the system is secure in handling sensitive information.

7.3.2.2 Qualitative results

The iterative prototyping team reviewed the test session videos to identify areas where participants struggled to complete tasks, expressed dissatisfaction with the demo, or made suggestions for improvement. Problems uncovered in iteration 2 testing include:

- Lack of user feedback for key interactions
- Important operationally relevant information that is missing
- Software bugs and glitches

The table at the end of this chapter (Table **10**) summarizes these findings and includes recommendations for how these issues might be addressed in the next design iteration. Each recommendation in Table **10** includes the evidence on which it is based and a priority rating. Priority scores in Table **10** are an estimate of the issue's importance to field operations and were based on the frequency with which the issue came up in test sessions and the degree to which it inhibited users in moving through the test case. These scores do not take technical feasibility into account.

Findings and recommendations are grouped by the functional component of the demo exercised during the test case (calendar/planning widget, mission planning widget,

communication widget, and map widget) with additional sections for prevalent themes in the data that were irrespective of any particular component (roles, capabilities, and staffing, ICAM/IDAM). Some items within these sections are labeled as requiring further investigation.

We are in the process of consulting with the broader project team that comprises sponsors, software developers, designers, and researchers, to do a cost/feasibility analysis of implementing recommended changes to the planning and scheduling tools. Then, we will prioritize issues to be designed into the demo, developed, and tested in future iterations based on both priority to the field and feasibility/difficulty of implementation.

7.3.3 Ongoing Activity and the Way Forward

In the following section, we discuss a number of high priority issues uncovered during the testing activity that require further investigation and therefore will likely guide future iterations of the design-develop-evaluate cycle. The most significant of these are related to roles, capabilities and communication. An additional issue flagged by the testing activity is the evolution of access and authority over time as plans transition from the planning to the monitoring/execution phase. We discuss the benefit of the HCD method toward socializing design concepts to the intended user community and plans for future iteration. We conclude this section with a high-level overview of how the iterative design team plans to move forward.

7.3.3.1 Roles, capabilities, and staffing

The need for planners to have ready access to information on partner operators' capabilities and availability as they are making planning decisions came up in both of our design iterations. In the first iteration, we added a simple drop-down menu that allowed users to assign staff to resources. This generated a great deal of user feedback and considerations for including staffing information in IMDE/CSS. This feedback suggests that for users at the LLE and USCG station level, IMDE/CSS planning and scheduling tools will not prove useful unless they provide ready access to this information. However, through our work to articulate the planning and scheduling use case, we know that the problem of integrating staffing information into

IMDE/CSS is very complex. For example, staffing information at many agencies does not exist in an authoritative system and is not digital—it lives on a whiteboard. The fact that this information is not digital poses a challenge to linking current systems in use to the IMDE/CSS enterprise architecture, and manually entering these data would have a significant, yet currently unknown impact on user's workflow. Understanding the implications of integrating staffing data into the planning and scheduling capabilities requires further investigation.

Another challenge that requires further investigation is the fact that the capabilities of individual actors change over time. For example, an operator may fill a role under calm weather conditions, but under turbulent conditions, that operator would be excluded from fulfilling that role because they lack the necessary qualifications to operate a vessel in higher risk weather. Similarly, the availability of a vessel will change as its fatigue limit is met.

7.3.3.2 Communication

In general, when users encountered the need to contact others, they did not turn to the User Directory that was included in the demo for this purpose. Instead, they frequently pointed out places where the task of contacting colleagues or collaborators should be embedded in other planning/scheduling sub-processes (e.g., whenever I assign a resource to a mission, I need a quick way to notify the crew) and their decisions on who to contact are role-based and mission specific (e.g., I want to contact whoever is operating that boat that I see on the map right now).

Communication based on role-based access control (RBAC) is a concept of growing interest,[128, 129] as is attribute-based access control (ABAC) (see Section 8.5). Our findings reinforce the need for access and control that are not only based on roles and attributes, but are also mission-specific. In the safety and security service system, the roles of individual actors often need to be modified as missions are planned and completed. For example, a private security company might perform some security tasks for a mission, but local law enforcement might

[128] Sandhu, R., Future directions in role-based access control models, in Information Assurance in Computer Networks. 2001, Springer. p. 22-26.
[129] Sandhu, R., D. Ferraiolo, and R. Kuhn. The NIST model for role-based access control: towards a unified standard. in ACM workshop on Role-based access control. 2000.

perform these same tasks for a similar mission at a different location. Tools that support communication need to be dynamic and sensitive to shifting roles and the corresponding shifts in communication relationships.

7.3.3.3 Access and authority, from planning to execution/monitoring

Authority evolves as time passes and plans move from the planning to the scheduling and then to the execution stage. For example, the person who plans the mission may not be the same person or people who actually schedule the mission and then manage the execution of the plan. Our testing activity surfaced the need to develop business rules for transferring decision authority between planning vs. scheduling vs. execution/monitoring activities. Future iterations could evaluate the encoding of rules into the system that transfer authority to different people at different points in the business process, but such rules have yet to be articulated.

7.3.3.4 Socialization

In addition to the rich feedback on the usability and usefulness of the demo, the act of meeting with individual users and introducing them to the demo also begins the process of socializing the community to the design concepts. When we meet with users to demonstrate, envision, and enhance the design concept together, both the users and designers learn the potential of the concept to help users do their work. We received numerous positive comments about the demo and the direction of the design. Below are a few examples:

> *"I like being able to see what is going on in the region. Often times we build silos, so this kind of breaks down those siloes and gets us all integrated and working together. There are just so few marine assets out there, we really need to coordinate and plan this stuff in advance and let everyone know where we are at and what we are doing. I think this [referring to the demo] is probably something I would use." – Local Law Enforcement*

The comment above is from a user who was particularly interested in the inventory of neighboring agencies' resources and the availability of these resources. This user also appreciated that the map widget allowed him to visualize the planned geographic location of resources assigned to an upcoming mission.

> *"The more people that collaboratively use a program, the better it's going to be. If it's just the Coast Guard using it, well, we already have programs for that, but if you add these other Federal agencies, it becomes pretty big." – USCG Station*

For this USCG user, one of the things that makes the design concept attractive is that it is intended to facilitate information sharing among other Federal and non-federal agencies. He likened it to WatchKeeper in this regard, and lamented that WatchKeeper's usefulness is limited because he believes it is not widely used. This user went on to encourage MOISA et al. to ensure that the process for gaining access to the IMDE/CSS system is simpler than that required to access WatchKeeper, because he believes this will increase its chances of being more widely used.

The below two comments were from a user who saw the potential of the map and the calendar/scheduling widgets to support (and possibly eliminate) two tasks that are currently burdensome in the Sector Enforcement Division: (1) Gaining access to and combining the schedules of individual USCG Stations into a single Execution Order (ExOrd), and then making this ExOrd available Sector-wide and ensuring that the ExOrd stays up to date with the most current plans; and (2) completing Incident Action Plans (IAP) which includes gaining access to and combining the individual plans of USCG Stations and other participating Federal and non-federal agencies and developing a map representation of how the different participants' resources plan to be distributed geographically at the time the plan is executed.

"Really, if everyone had access to it, that literally takes six hours [of work] a week off of our shop per person, so, it's huge." – USCG Enforcement

"This is so many steps ahead of what we are currently doing—the opportunity to use something like this is just unfathomable right now. …there's no way we can get this by next week so we can start using it?" – USCG Enforcement

7.3.3.5 Plans for Moving Forward

Preliminary results of iterations 1 and 2 have been delivered to the software development group. The significant value of this information has been recognized by SRI International and the sponsors of the greater IMDE/CSS project (DHS). As a result, sponsors have recommended that the iterative prototyping team continue this activity into fiscal year 2016. The iterative prototyping team is currently developing a project plan for completing no less than four additional iterations in the design of IMDE/CSS planning and scheduling capabilities to be delivered as part of an operational demonstration in March 2016. The following is a high-level list of issues to be addressed in future iterations:

- Interagency resource management
- Support of mission flow from planning to scheduling to monitoring
- Transparency and access management of mission components
- Mission-based communication
- Geospatial components of planning and scheduling
- Deconfliction of multiple missions
- Mission staffing

The iterative prototyping team plans to help introduce, socialize and exercise the planning and scheduling service with the broader Puget Sound operational agencies and individuals in preparation for the Operational Demonstration. Finally, the iterative prototyping team plans to facilitate a discussion of the transition and adoption of the IMDE/CSS planning and scheduling capabilities, including ongoing regional system evolution beyond the operational demonstration.

Table 9: *Summary of results for quantitative post-test questionnaire* (N = 5)

	Strongly disagree 1	2	3	4	Strongly agree 5	N/A	Mean	% Agree*
1. Overall, I am satisfied with this version of the system			1	4			3.8	80%
2. I would recommend a system like this to a friend				4	1		4.2	100%
3. This system works the way I want it to work		2		2	1		2.6	60%
4. I feel I need to have a system like this		2		2	1		2.6	60%
5. A system like this is secure in handling sensitive information.						5	--	--
6. Overall, a system like this is trustworthy.				2		3	4	100%*
7. Agencies that partner with my own will have concerns about security, privacy, and confidentiality associated with a system like this.		1		2	2		4	80%
8. In general, I believe that partner agencies will be satisfied with a system like this.			2	3			3.6	60%
9. A system like this will contribute to my agency's ability to collaborate with partner agencies for improved mission accomplishment.			1	1	3		4.4	80%
10. A system like this would allow me to work with an appropriate level of sensitivity to others' need for information sharing and safeguarding.			1	3		1	3.75	75%
11. If I had access to a system like this at work, I would use it.		1		2	2		4	80%
12. If a system like this were available, it would be helpful for my agency and agency partners.				2	3		4.6	100%

*This percentage is based on responses from the two participants who answered this question. Three of the five participants felt that they did not have enough information to answer this question.

Table 10: *Preliminary summary of areas for improvement and design recommendations*

Preliminary summary of areas for improvement and design recommendations				
Finding/User Comment		**Recommendation**	**Priority**	**Difficulty**
MAP WIDGET				
· The planned transit route of a mission (including drop-off points and stops) is critical to decision-making about where one's own resources might be needed and in what timeframe.		1. Add simple GIS drawing tools and geo-fencing. Recommend borrowing these from WatchKeeper.	High	
· Information on jurisdictional boundaries is important to planners' decision-making.		2. Add map layers that can be toggled on and off showing USCG station boundaries, shipping and traffic lanes, county lines, etc.	Med	
· Users want to see resources mapped by mission, by agency, by resource type.		3. Add filters that allow people to see resources on the map by mission, agency, and resource type.	Med	
· When you hover the mouse over a resource, you get information re: to which mission a resource is assigned. a) This does not currently add value because the current design only allows users to look at a map for a single mission and only shows users resources assigned to the open mission. b) However, users indicated that it is useful for them to look at the maps for more than one mission at a time, overlaying one map on top of the other.		4. a) Allow users to use filters (mentioned in above comment) to view maps for more than one mission at a time. b) Include resource agency and type in information that comes up when you hover over resource on map.	Med	
· Users need feedback that tells them that newly assigned resources appear on the map. Many did not notice this, which brings the risk that they will leave the resource at its default starting position rather than moving it to its accurate starting position. Also, moving resources around on a map is not always critical for single agency operations at the LLE or USCG station level, so adjusting the position of resources on a map was not intuitive to all users.		5. When a new resource is assigned, users should be notified that an icon representing the resource has appeared on the map, and they should be prompted to move it to the correct position, or they should be given the option of adding the resource to the map and adjusting its position. We need to ask users to help us envision a design that will be intuitive to them.	High	Requires further study
· Users need feedback that tells them when multiple resources are stacked on top of one another—users often mistook a stack of resources for a single resource.		6. When resources stack up on the map, add a label that indicates the number of stacked resources.	Med	
· Need more descriptive icons		7. Consider borrowing iconography from WatchKeeper and/or WACOP.	High	Requires further study
		8. Add the ability to set trip lines in planning so that during execution, users will get a notification when certain vessels cross the trip line on the map. This capability is currently available in WACOP's Command Bridge app.	Low	

		9. Eliminate artificial stack of new resources at Victoria – each resource should either have a default starting position or appear in an off-the-map holding pen from which it can be moved onto the map. We need to ask users to help us envision what a design that will be intuitive to them. (See item 5 above)	High	Requires further study
ROLES, CAPABILITIES, AND STAFFING				
NOTE: A system to aid in single-agency planning day-to-day should support planners' decision-making regarding their resources' capabilities as well as availability. Because capability is often a combination of resources (e.g., a piece of equipment and a person who is trained to operate it), planners need to have information on personnel and equipment integrated with information on vessel schedules.				Requires further study
· Planners make staffing decisions based on whether certain crewmembers have the right training and qualifications to use certain resource capabilities (e.g., Rad/nuc detection equipment) or perform certain operations (e.g., diving).		1. In resource details, consider adding what skills and training are needed to operate the resource. This should link to a database that holds personnel training information. Such a system could support decision making about which crew to assign to a resource or mission by narrowing the list of crewmembers by availability AND *capability*. This requires adding rules re: the training and skills required to undertake certain missions and operate resources.	High	Requires further study
· Planers make decisions based on whether the operational roles played by assigned resources are sufficient to carry out the mission and whether they have the right capabilities to do the job. Just knowing the number and types of resources that have been assigned is not enough information to support decision-making.		2. Consider giving mission authors the option to specify what capabilities are needed when they create the mission, include resource capabilities in resources properties sheet, and consider giving users the option to specify what role a resource will fill when assigning it to a mission. Users reported that USCG and LLE in Puget Sound rely on the same taxonomy for the different operational roles. The system could support decision making by narrowing lists of available resources based on resource availability AND capability.	High	Requires further study
· Planners consider resource fatigue limits in their decision-making.		3. Add rules to encode fatigue limits into resource inventory. As resource fatigue limits will change as time progresses and weather changes, this will need to be tied to business rules that have yet to be articulated.	Low	Requires further study
· Users need to be able to assign more than one crewmember at a time.		4. Either have check boxes next to crewmember names, or add the ability to hold command and select more than one crewmember before clicking "assign."	Med	
· Often, the same people are scheduled to crew together for weeks at a time.		5. Users need the ability to create and assign set crew groups.	Low	
		6. Make it so that a person cannot be staffed to a resource more than once	High	

		7. Staff capability should be linked to weather data so that if the weather requires a certain level of training to be able to operate the vessel, the system will prevent you from assigning staff who are not qualified to operate a vessel at that time. USCG has a training management system that may be the authoritative system that holds info on qualifications.	Low	Requires further study
CALENDAR AND PLANNING WIDGET				
NOTE: Advanced planning and response planning exist at different points along a continuum from long-range plans to what is happening right now. Both activities require the same types of information: What is the entity, where is it and in what condition, what is the activity that needs to be performed on the entity, what resources are needed, and when can they be brought to bear on the activity? What distinguishes the information in an advance planning vs. response scenario is the value of the information attribute. The finding that planning for events that are both emergent and planned in advance rely on common information types suggests that a single tool or process could be designed to support planning activities anywhere along the continuum of pre-planned to emergent events.			High	Requires further study
· Users found it difficult to locate their own agency and resources within the long list of agencies and resources. Also, the way resources are listed at the same hierarchical level directly below their agency means that users are frequently looking at a list of resources while the agency to which they belong is off-screen. This makes it difficult for users to recall at which agency's resources they are looking.		1. Resource lists should be nested within the agency list. Borrow the nested list convention from the mission view. I.e., clicking on a black triangle below the agency name will open that agency's resource list. We may want to add more levels to the list hierarchy down the road. E.g., USCG Sector>USCG Station>Station resources	High	
· Users were confused when they could no longer find a resource in the resource list when it disappeared because it had been assigned to a mission that was open.		2. I believe the purpose of this function is to prevent users from scheduling the same resource more than once. Instead of removing the resource from users' view, add deconfliction. Give them a warning message if they try to schedule the same resource to the same mission more than once – similar to iCal or outlook.	High	
· Users did not get adequate feedback that they had successfully assigned a resource to a mission.		3. Rather than removing the resource from the list of available resources once it is scheduled, the mission should appear on that resource's schedule in the resource list. Users should be able to see that the resource has successfully been scheduled to the mission without needing to "close" the mission in the mission pane.	High	
· To assign a resource to a mission, users frequently tried to drag resources onto the mission name or elsewhere in the mission row outside of the scheduled time window.		4. Allow users to assign a resource to a mission by dragging and dropping the resource to anywhere within the mission row.	Med	

· Users need a way to assess resource availability at a glance.		5. Color code resource names so that resource status on the current day is clear. Alpha = underway and available; Bravo = at the pier and available in a few hours; Charlie = unavailable due to maintenance and repairs. As resource status will change as time progresses (i.e., transition from planning to execution), this will need to be tied to business rules that have yet to be articulated.	High	Requires further study
· Users need the ability to assign a resource to only a fraction of the total mission duration.		6. Allow users to click and drag mission start and end times for a particular resource. Similar to how Apple's iCal app allows you to adjust event start and end times.	High	
· The clock was difficult for users to read.		7. Put time clock in military time and allow users to select what time window they would like to view. Extend schedule grid lines up to the hours at the top of the grid and add tick lines for 30m intervals.	Med	
· Opening and closing missions appears to jump the user to the top of the resources list, so that they lose their place.		8. This is probably a bug that needs fixing?	Med	
· Users need an easy way to un-assign resources from the planning page.		9. Use the same interaction that they use to assign the mission—click and drag resource from mission pane back up to resource pane.	Med	
· Users frequently need to reassign scheduled resources to emergent missions of higher priority.		10. Currently, it appears as though the only way to unassign a resource to a mission is by going into the mission details and removing the resource from the assigned resources. Users should be able to drag a resource to the higher priority mission and deal with the reassignment via a deconfliction function. E.g. when an assigned resource is dragged (reassigned) to the new, higher priority mission, users see a dialogue box that prompts them to deconflict. E.g., "Resource X is already assigned to mission Y. Do you wish to reassign resource X to mission Z? Click OK or Cancel."	High	
· Information on the weather forecast influences planners decision-making on crew assignment and which resources to use.		11. Add a live feed of NOAA's hourly weather forecast at the top of the schedule in the planning pane.	Low	
· Double clicking on a resource opens duplicate resource property sheets; double clicking on the mission opens duplicate mission details.		12. Fix so that only a single instance of a resource property sheet can exist at a time; fix so that only a single instance of mission details can exist at a time.	High	
· User wanted to able to see more of the mission or to make the mission view larger.		13. Split screen option does not give you a way to see the mission list in full screen. Consider having the split screen be the default state and then borrow the convention from most office applications: two buttons in an upper corner of each view—one that makes the view full screen and one that minimizes the view.	High	

· Users need a way to assess mission priority at a glance.		14. Consider encoding mission risk into the visual representation of missions in both mission and resource panes. Not color, as it may be used to represent resource status (gradient?). Will need to check with users re: variables that allow them to determine priority-risk, a combo of multiple variables?	Med	Requires further study
· Finding desired missions and resources in the mission and resource lists was challenging, even with the limited number in in the demo—in reality people will need to sort through many more.		15. People need a shortcut to search for specific mission related information. Consider adding a search box so that people can search for missions, resources, agencies, etc. by name.	Med	
· Planners need to be able to schedule a resource for more than one mission in a day.		16. Add this functionality.	High	
		17. When a mission is open, the blue bar on the schedule for the resources assigned to that mission repeats the resource name. Replace resource name here with the role of the resource. This requires the agreement on a standard set of roles to which a resource can be assigned.	Low	Requires further study
		18. Reduce whitespace by decreasing row height.	High	
		19. In the future, it will be useful to be able to export events to Outlook, iCal, and Google calendars	Low	
· Who has authority and access to mission information changes over time as missions move from the planning stage into monitoring and execution.		20. Consider developing business rules for transferring decision authority between planning vs. monitoring emergent activities. Maybe once the rules are set, they are encoded into the system and it transfers editing authority to person at different place in business process.	Med	Requires further study
· Users may need to add civilian agencies and resources to the inventory for a single mission.			Low	Requires further study
COMMUNICATION WIDGET				
NOTE: In general, when users encountered the need to contact others, they did not turn to the directory. Instead, they frequently pointed out places where the task of contacting colleagues or collaborators is embedded in other planning/scheduling sub-processes (e.g., whenever I assign a resource to a mission, I need a quick to notify the crew) and their decisions on who to contact are role-based and mission specific (e.g., I want to contact whoever is operating that boat that I see on the map right now).			High	Requires further study
· Users wanted to know the status of people in the directory. I.e., are they online now and available to chat?		1. Consider borrowing Facebook's convention of a green dot showing who is online now and also indicating how long it has been since a user logged in.	Med	

· Users need multiple communication options. They need to be able to chat, send email, make a phone call, or send a text (if contact number is a cell number).		2. Add these communication options in the user directory. Consider borrowing design from Apple iPhone "contact" design.	Med	
· When a resource is assigned or re-assigned, planners need a quick way to notify others of the schedule change.		3. Add ability to quickly notify assigned crew of schedule changes. Consider borrowing from other calendar apps (iCal, Google, etc.) in the way making a change to event details gives you a pop-up that allows you to notify event invitees.	Med	
· Users want the ability to push notifications of newly completed plans and plan changes to specific other users who may or may not be assigned to the mission.				
· Being able to look on a map and have a direct line of communication to a POC who is either (a) responsible for planning/coordinating the resource or (b) on/operating the resource at a specific location is very useful. The ability to do this real-time using AIS data is reportedly available in other applications (Spillman).		4. Consider adding the ability to click on a resource on the map to bring up an option to communicate with the POC for that resource. This needs to evolve in association with business rules about who has authority during planning vs. execution. E.g., in planning, it is important to connect with the planner or coordinator; in execution it may be important to connect with who is actually on the boat in real time.	Med	Requires further study
MISSION PLANNING				
· Users want to see which crewmembers have been assigned to a mission in the mission details.		1. Once staff are assigned to a resource, this should update to an auto-generated list that appears in the mission details, or add a way for users to see or link to staffing details. This needs to include who the people are and their training and qualifications.	Med	Requires further study
· The meaning of the resource ID numbers appearing in the unlabeled "assigned resources" box was unclear to users.		2. Label the "assigned resources" text box and include what number of resources is assigned out of what number requested. (Use #/# convention from mission pane.)	High	
· Users wanted to be able to bring up resource details from the mission information		3. Make it possible to open resource details by clicking on resource in the list of assigned resources in mission details.	Low	
		4. Fix bug so that a newly assigned resource shows up in mission details without needing to close and reopen mission details.	High	
		5. Consider adding a way for users to view mission editing history so that they can see who authored and edited the mission and when changes were made. Link this to user directory/contact information.	Low	
		6. Add capability to plan at varying levels of detail—operational AND tactical planning.	Med	Requires further study
		7. We may need three or four tiers in a hierarchy of events: Big event, operations required to pull off the event, missions that comprise the operations, and then sorties that comprise the missions.	Med	Requires further study

ICAM/IDAM				
· Users manipulate resources in different ways while they explore different planning and scheduling options (draft plans) before deciding on a final plan. It is this final plan that they typically need to share with others.* *Although it didn't come up un these interviews, it is possible that planners would like to share draft plans with specific individuals who are aiding in the planning process.		1. In the current design, there is no distinction between when a plan is in the process of being constructed and when it is complete. Consider adding a way for users to work on a plan and schedule and explore different options in a planning workbench mode and then "publish" the plan once it is complete. Users also need to revise completed plans, so they need to be able to return to working on a plan in the workbench mode and publish updates.		Requires further study
· Users felt unsure about inputting their own plans and schedules because they did not have an idea as to who else could see their information and what their own plans might look like to other users (within and external to their agency) with varying levels of access/permission.		2. Consider adding a way for users to see their own plans from other's perspectives. Consider borrowing Facebook's design concept that allows you to select an option to look at your own profile from the perspective of other categories of users (friends, the public, etc.).		Requires further study
· Users need visibility into the underlying permissions that govern others' access to their information, both within their own agency and in partnering agencies.				Requires further study
· Users need an easy way to grant other individuals access to completed plans from within the planning and scheduling module.				Requires further study
· Users need the ability to grant access and authority to other users for specific missions. Some of these users may be private security contractors who do not typically use IMDE/CSS. This mission-specific access and authority needs to dissolve once the mission is completed.				Requires further study

8 Repeatable Mechanisms

Coordination and collaboration among a diverse set of stakeholders is critical to the success of safety and security operations. One of the findings to come out of year one of the MOISA project was a need for repeatable collaborative mechanisms that would facilitate information sharing and collaboration between the Federal government and the Puget Sound maritime community. Furthermore it was identified that these repeatable collaborative mechanisms should focus on standards, policy, technology, information sharing, use case business processes, interoperability, integration, and solution development. Therefore, during year two of the MOISA project, we again sought input from the Puget Sound maritime community to identify the repeatable mechanisms needed to improve collaboration within the FSLTIPP community. This section describes six repeatable collaborative mechanisms from year two of the MOISA project.

8.1 Center for Collaborative Systems for Safety Security and Regional Resilience (CoSSaR)

The Center for Collaborative Systems for Security, Safety, and Regional Resilience (CoSSaR) is an organization created to lead innovation in the design, development and use of collaborative systems that support regional operations for security, safety and resilience in the Puget Sound region. The center is a multi-disciplinary facility and environment where professionals hailing from a wide range of entities team with university experts to align strategies, processes, and investments in systems for security, safety and resilience.

CoSSaR has become the institutional home for MOISA and related projects, building on the MOISA year one exploration of the complex daily operational information-sharing environment of the Puget Sound safety and security community. MOISA's second year has leveraged the CoSSaR "umbrella" in its identification and exploration of potential ISE interventions to enhance the information-sharing environment and facilitate alignment of Federal investments in maritime safety and security. One facet of MOISA's leverage of CoSSaR

is the establishment of a Co-Development Lab.

CoSSaR's Co-development Lab facilitates the regional security and safety community in their efforts to define and evaluate collaborative processes and the desired information-sharing environment to support these processes. This facility is housed in the Center for Environmental and Information Systems (CEIS) at UW's Applied Physics Laboratory. As a Department of Defense designated University Affiliated Research Center (UARC), the APL has both the charter and infrastructure to create collaborative teams among experts in academia, government, and industry. By being a DoD designated UARC they have the capabilities to work with classified (up to TS/SCI) and controlled unclassified information (CUI). Inside the APL's 132,344 square feet is a command center/visualization room for evaluation of situational awareness tools and displays.

The CoSSaR center is equipped to lead the development and implementation of repeatable collaborative mechanisms through which the Federal government can improve collaboration with the Puget Sound region. The long-term stewardship provided by the center allows CoSSaR to act as a force multiplier, increasing the value of individual projects like MOISA by enabling the findings to be maintained and applied to a wide range of safety, security, and resilience activities across the FSLTIPP. For example, the Puget Sound Sensor Survey and associated Sensor Workshop Analysis (see Section 4) – carried out as a part of MOISA 2 research – will live and be maintained in a CoSSaR information repository long after the completion of the MOISA 2 project, informing and enabling future information sharing efforts across the Puget Sound region. The remainder of this chapter describes the repeatable collaborative mechanisms that have been identified, explored, and, in some cases, implemented during year two of the MOISA project.

8.2 MOISA Standards Use and Extensions for Repeatable Mechanisms

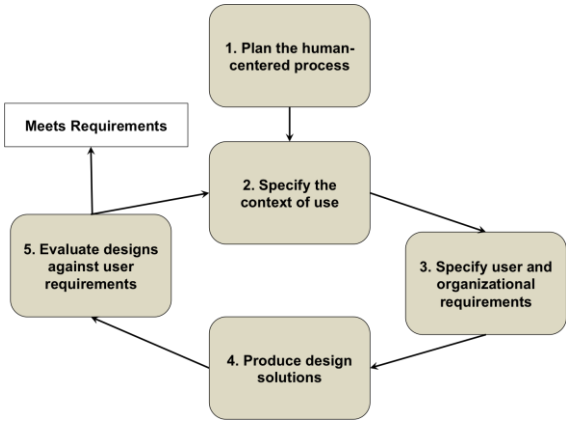
Standards provide the foundation for many repeatable mechanisms, especially in the realm of Information technology (IT) where standards can cover hardware, software or methods. Two of

the most widely respected standards bodies in this area are the International Organization for Standardization (ISO) and the Object Management Group (OMG). MOISA has interacted with both of these groups, especially OMG, and is applying the following standards to the development of enhanced ISE systems:

- ISO: 9241-210, *Human-Centered Design for Interactive Systems* specifies the top-level method for developing systems that are both useful and usable.
- ISO: 25062, *Common Industry Format for Usability Test Reports* (CIF) specifies the contents of reports of tests, thereby setting requirements for the planning and conduct of the tests as well.
- OMG: Business Process Modeling Notation 2.0 (BPMN) specifies the modeling language to analyze and develop IT requirements. BPMN is intended to model use cases for organizational work that is supported by computing but also includes substantial activity that is performed manually.

These three standards provided the methodical activity patterns needed to begin user-centered design for MOISA. As shown in *Figure 13*, the Human-Centered Design standard specifies how iterative prototyping refines requirements on the basis of evaluation. The CIF for usability testing is considered "the gold standard" for evaluation to satisfy Human-Centered Design of user interfaces (step 5). Together they form a widely followed paradigm for creating interactive systems that are both usable and useful because they address organizational requirements as well as those for individual users.

Figure 13: ISO Standard Method for Human-Centered Design Method



In their best origin, methods standards are the codification of practice that has proven successful for important situations that should be repeated as the default for those situations. Although they provide the default, standards must continue to evolve in order to remain valuable. MOISA personnel played leading roles in the original development of the CIF and continue to consult with US National Institute of Standards for its adaptation to security-critical and health-critical systems.

The BPMN standard addresses steps 2 and 3 of Human Centered Design, which can be refined, but not discovered with iterative prototyping. It has been implemented in over three-dozen commercially supported modeling tools. The tools are widely used to model and analyze how IT should be applied to improve operations/business processes. MOISA 1 applied a BPMN-based modeling tool to demonstrate how it could capture the usage and change of security related information in the processes of a mid-sized commercial cargo terminal in a large port. This model continued to be of use during MOISA 2 and was presented to the Standards Coordinating Council, chaired by the PM-ISE, at the September 2015 OMG meetings.

The software tool that MOISA applied to model security information used by the terminal included several innovations to improve over the standard that make it highly relevant to emerging needs for interoperability requirements that are both accurate and economical. Following a series of presentations and demonstrations to Victor Harrison, Executive Vice-President of OMG, MOISA gave four specially scheduled presentations at the September 2015 OMG Technical Meeting held in Cambridge, Massachusetts. One purpose of the presentations was to illustrate the value of the innovations and the simplicity to extend the BPMN standard to include them.

Essentially, the BPMN standard was extended to integrate modeling the use and change of information in the context of operations. The innovation accomplishes this by treating information resources as a peer of other physical resources, such as labor or equipment. The innovation includes an editor to enter the information and the resource that provides it as properties of the tasks that make up a business process. For very little additional effort, a BPMN analyst can add the information as part of developing the model.

When the model is complete, the tool automatically creates an information dictionary. This dictionary lists the information that is needed to support the enterprise, and only that information that is actually used or changed. So it brings precision and economy to interoperability requirements. The dictionary also associates each information element with the resource that provided it. So it also provides a more complete specification for interoperability requirements. The benefits should include:

- Important relationships among information elements
- Greater precision and less cost for JIT
- The important relationship between operational improvements and IT
- Less clutter for users of security information systems
- Physical information resources for understanding of the entire flow, and analyzing them as candidates for IT systems
- User participation and buy-in

Two MOISA team members have been invited to join the Standards Coordinating Committee as voting members. Through participation, MOISA will influence the adoption of standards for effective interoperability that our studies have identified as key, and to "build in" usability and usefulness to safety, security and resilience-related systems.

8.3 Coordinated Regional Survey Mechanism

The coordination and collaboration of information by a diverse set of stakeholders is critical to the success of safety and security operations, yet information sharing can often feel like a burden. For the individual providing information, he or she may not know how to get the information or it may have been provided to some other agency previously. Alternatively the surveyor or requestor may be aware that the information exists somewhere, but it may not be in a format that is useful or accessible, or they may not know who to ask for it. For some, the burden may be in the number of requests for information they receive. Perhaps individuals get requests for information that they do not possess or perhaps they are not familiar with the individual requesting the information and therefore are reluctant to share it.

A coordinated regional survey mechanism could help to alleviate the burden of requests for information (RFI) and information gathering tasks (e.g., surveys, plan updates, etc.). To explore this possibility, we began by interviewing a number of individuals who are either responsible for gathering information or for responding to requests for information. Our goal was to better understand how a coordinated regional survey mechanism could alleviate the burden of information gathering and information sharing. The sections that follow detail our approach, findings and recommendations.[130]

8.3.1 Approach

We began our background research into a regional coordinated survey capability by obtaining, from project sponsors, examples of RFIs and surveys that were used by various agencies in the past few years (see Appendix E, Table A). Using snowball sampling[131] and these initial examples, we were able to identify thirteen other individuals who were responsible for either creating RFIs or surveys (i.e., surveyors) or who were responsible for responding to these documents (respondents). We then prepared a protocol (see Appendix E, Table B) for surveyors and respondents to assist us in addressing the following questions:

1. What are the information gaps in current survey/RFI processes?
2. What are some strategies for ameliorating these gaps?
3. What are the organizational, technical, and policy requirements for implementing these strategies?

[130] We are aware that some individuals view surveys as separate from requests for information (RFI) where the former represents a vehicle for soliciting opinions while the latter represents a vehicle for soliciting facts. Therefore, while we refer throughout this report to a survey mechanism, we intend for the proposed coordinating mechanism to be utilized for both surveys and RFIs.

[131] "Snowball sampling is 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

8.3.2 Findings

We conducted seven telephone interviews (see Appendix E, Table C) with individuals who were surveyors, respondents, or both. From these interviews, we identified the following problems:

8.3.2.1 Visibility of Information Gathering Activity

There is very little visibility into all of the different survey and information gathering activities (updating plans, etc.) that are happening concurrently and how these information-gathering activities might overlap. This problem has two primary symptoms. First, entities requesting information miss out on opportunities to collaborate or share information with one another; instead they often approach the same individual multiple times for the same information. Second, respondents who do not know the information requestor or are not aware of the purpose of or history behind an incoming request for information are reluctant to respond, as it is time consuming to "vet" the requestor and confirm the legitimacy of the request. This lack of response forces the surveyor to request the information again of the same person or send out the RFI or survey to another individual in hopes of getting a response.

8.3.2.2 Appropriate Request Processes

Requests for information and surveys often do not follow the "appropriate" process. For example, for Terminals and Ports, the United States Coast Guard (USCG) has regulatory authority, so when a terminal or a Port gets a request without first having heard that the activity is sanctioned by USCG, they will not immediately respond to the request. They will delay response so that they can first vet the activity with someone at the USCG (see *Visibility of Information Gathering Activity* above). If all requests were consistently vetted by USCG first, and if terminals/Ports are made aware that the activity is vetted before the request gets to the facility, then this would alleviate the burden of respondents doing their own vetting.

8.3.2.3 Correct Contact

Information requests do not always target the appropriate people. In this case "appropriate" means people who are interested and invested in responding, or people who have some responsibility to give a response. This is particularly important for optional RFIs where knowing which individual in an organization is passionate about the issue and interested in the results is critical to getting a response. Several interviewees mentioned that this was the most time consuming step in the RFI and survey process.

8.3.2.4 Results in a Timely Manner or Useable Format

Results are not sent out in a timely manner and if they are, they are not in a format that is useful to the majority of users. In addition, sensitive data may need to be password protected or encrypted such that only appropriate personnel can access the results.

8.3.3 Recommendations

The solutions that follow address the problems that we learned about during our interviews. Further work, described in the next section, is necessary to determine functional as well as technical requirements.

8.3.3.1 Promoting Visibility

An organization like CoSSaR could act as the point of contact for anyone seeking information in the region. CoSSaR could also be responsible for promoting a public information campaign to raise awareness of the "appropriate" process for requesting information. In other words, CoSSaR could offer an information request service to all agencies; however, funding this service and incentivizing Federal agencies (whose target survey respondents are mandated to respond) to go through CoSSaR are some issues that would need to be addressed.

8.3.3.2 Central Contact Repository

One of the interviewees suggested that each agency designate a Chief Information Officer (CIO)

to handle all requests for information and surveys. While this solution may resolve the problems concerning whom to contact to provide information or opinions, a more practical alternative may be to have the Captain of the Port promote voluntary CIO subcommittees at the AMSC and the Puget Sound Harbor Safety Committee. CoSSaR could then help to advise these subcommittees and funnel requests for information and surveys through these committees. CoSSaR could also be responsible for maintaining this contact list and making it available to surveyors.

8.3.3.3 Central Results Repository

A newsletter informing individuals about the information gathering activities that have been conducted in the past few months and informing individuals of upcoming RFIs could be published on the CoSSaR website and also distributed to those individuals who indicated the need for information. The newsletter would include information on where and how to obtain results from past activities information gathering activities. In addition, a standard results repository could serve to meet future requester needs without bothering operational agencies. Finally, a central results repository could become a valuable regional information source and support future analyses requested by the community.

8.3.3.4 Standardized Tools and Processes

As Washington is a Home Rule State, mandating a standardized tool or process is not possible, and there are significant barriers to designing standards in a community of diverse stakeholders operating under different governance models and within different cultural, political, and technical constraints. We encountered one successful example of a standardized information sharing process across all regional FSLTIPP sectors. King County Emergency Management uses a standardized form and process to collect information from entities all over the region in the event of a crisis. To meet the needs of regional stakeholders with varying technological capabilities, the form is an editable PDF that can be transmitted electronically via email or fax and can also be distributed and filled out via snail mail. Responses received electronically can be automatically uploaded to a central database, and King County Emergency Management has

staffing and budget to record data submitted via paper forms. Although the use of this standardized form cannot be mandated, information providers are incentivized to provide this information because it is only used in emergency situations as a part of incident response. Our prior research has shown that individual information sharing practices and priorities differ for day-to-day versus incident focused operations, so although this success story is encouraging, it is not clear that adopting a similar standardized process and form to support day-to-day information gathering activities would be similarly successful; however, it is worth further discussion and consideration.

8.3.3.5 Technical Capabilities

An electronic survey tool does not appear to be necessary as four of the interviewees said that information requests looking for an electronic response typically received a low response rate. However, a database where a surveyor could compare the information available to what is needed would be helpful in reducing duplicate effort on the part of the surveyor and respondent. Any technical requirements for how a database would be populated, maintained, and made accessible (i.e., what type of security measures would need to be in place) must be determined. With respect to populating the database, many of the current RFI and survey efforts are done via face-to-face meetings and are recorded on paper, and not input into a database for analysis but are instead directly translated into narrative reports or documents. Therefore, how to input these narratives into a searchable database, including who would be responsible for conducting and funding this work must be determined. One solution to the issue of security could be to fund CoSSaR to run queries and then generate reports for people requesting information, and then only CoSSaR would need to have authorization to access the database[132].

[132] Possible reference model - the VA has a data warehouse and a small staff of people who will run queries for interested researchers, sometimes for free, sometimes for a fee. How to staff and fund CoSSaR to perform these queries is an open issue that needs to be resolved.
http://www.hsrd.research.va.gov/for_researchers/vinci/cdw.cfm,
http://www.hsrd.research.va.gov/for_researchers/vinci/default.cfm

Some RFI and survey results are currently posted to HomePort[133]; however, several people complained that the site is difficult to access. One potential solution may be to improve access and information organization on Homeport. As an example of improved access, some interviewees suggested that providing individuals with an actual link to the results rather than simply stating they were available "somewhere" on Homeport would make it more convenient and less time consuming to access results.

HSIN was not specifically identified by any of our interviewees as a repository of RFI or survey results. Given the high volume of users (see Section 5.5) and its ability to share "Sensitive But Unclassified (SBU)" data over a secure channel (see Section 5.4), HSIN could be used in this capacity; however, further research is required.

8.3.4 The Way Forward

The activities outlined below should be conducted prior to development of a coordinate survey mechanism. Funding to conduct this analysis and subsequent development will require outside funding.

- Analyze organizational barriers and policy constraints associated with a regional coordinated survey mechanism.
- Analyze technical requirements for implementing and maintaining a survey mechanism.
- Analyze cost/benefit and/or feasibility of housing and maintaining a standardized survey mechanism at CoSSaR.
- Coordinate a workshop inviting interested parties to get their feedback on the following:
    - Given the concerns identified above, is a regional survey resource something that the community wants/needs?
    - If so, how might the above concerns be addressed?
    - Are there any concerns/considerations that we have not yet identified?

[133] Homeport is a United States Coast Guard system, but organizations that in a community of interest working with the Coast Guard are allowed access.

    - What are the recurring surveys/data collection efforts and with what frequency do they recur?
- Coordinate the co-design of a workshop to further develop and evaluate the following ideas:
    - Using CoSSaR as a distribution center.
    - Creating a contact list of RFI/survey recipients.
    - Assigning a CIO per agency as the initial contact for all surveys/RFI.
    - Determine dissemination avenues, survey formats, and security levels.
- Analyze how CoSSaR can be used to facilitate data collection and address the following:
    - Contact list maintenance
    - Procedures/standards for how respondents are contacted, question format, etc.
    - Results repository maintenance
    - Data analysis requirements

8.4 Controlled Unclassified Information and the Safety and Security Community

A major goal of the MOISA project is to enable responsible information sharing within the maritime Information Sharing Environment (ISE) in the Puget Sound region – and to provide insights that may be replicated in other regions and nationally. During the first year of the MOISA project, researchers encountered unexpected challenges to information sharing in the form of restrictions on the distribution of federal Controlled Unclassified Information. For many state and local safety and security personnel, the rules associated with sensitive federal information are not familiar, and the MOISA team was no different.

Confusion regarding the rules and restrictions associated with controlled unclassified information can result in the risk of divulging sensitive information or, more likely, it can discourage legitimate and necessary sharing because personnel do not want to risk violating the rules. To encourage appropriate and responsible information sharing, MOISA has developed a guide for identifying and handling federal sensitive information as a repeatable mechanism to

enable responsible information sharing throughout the Puget Sound region and beyond. That guide is provided as Appendix G:.

8.5 Project Interoperability: Potential Use of Federal Data Standards

MOISA Year Two reviewed a set of emerging Federal data standards as listed under the Project Interoperability website, developed by the Program Manager of the Information Sharing Environment (PM-ISE) for potential use in improving identification and information management to enhance mission goals.[134]

> "Information interoperability is the ability to transfer and use information in a consistent, efficient way across multiple organizations and IT systems to accomplish operational missions. From a technical perspective, interoperability is developed through the consistent application of design principles and design standards to address a specific mission problem."[135] – Project Interoperability website

One of MOISA's goals is to facilitate information sharing among various organizations with different missions and resources. The two main components of information sharing are building trust-based relationships to encourage information sharing and developing the technical capabilities to efficiently and securely share agreed upon information that can be replicated across FSLTIPP agencies. Much of MOISA's work through its second year has been focused on the former. MOISA's third year will expand to help willing partners facilitate automated information exchange.

[134] Project Interoperability website http://project-interoperability.github.io/ accessed 7/17/15.
[135] Ibid.

PM-ISE's Project Interoperability draws from ten main information-sharing tools, each of which could be considered a repeatable mechanism to facilitate timely and responsible information sharing throughout the Puget Sound region and across the FSLTIPP community. A description of these tools can be found at http://project-interoperability.github.io/. Future work will build on this initial analysis to examine how interoperability tools and concepts are useful and applicable to mission accomplishment; discuss why some tools may not be useful; and recommend strategies to improve tool design, usability, and outreach.

9 Discussion and Conclusions

> *Without a process to obtain and incorporate port-partner input into the development of future WatchKeeper requirements, the Coast Guard does not have reasonable assurance that WatchKeeper will satisfy port partners' needs, and facilitate mission-based information sharing to achieve the goals of the IOC project.*[136]
>
> Government Accountability Office (GAO), 2012

MOISA 2 was about facilitating mission-based information sharing. Of course there were products, including:

- the first iteration of a regional sensor survey (Section 4)
- the outcomes of community workshops that analyzed opportunities for enhanced mission accomplishment through increased sensor sharing (Section 4)
- an analysis of current systems that impact the regional ISE and their relationship to an IMDE/CSS enterprise architecture based on an open widget framework (Section 5)
- an analysis of two mission-based use cases—suspicious small vessel security and operational planning and scheduling (Section 6)
- a variety of collaborative mechanisms, including: a new regional center to provide a shared resource for co-design and development of regional systems; a guide for the handling of controlled unclassified information by non-federal organizations; and exploration of a shared survey mechanism (Section 8)

These products were extremely valuable in their own right. The sensor survey, for example, was initiated in response to a desire expressed at the Puget Sound Area Maritime Security Committee (AMSC) for such a regional resource. The series of community workshops which followed to explore the potential of sharing sensors and other regional data to enhance mission accomplishment uncovered important opportunities, as well as difficult challenges to address if those opportunities were to be realized. Key workshop takeaways such as the increased

[136] United States Government Accountability Office (GAO), "GAO-12-202: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers," 2012.

importance of mobile sensors, the desire for increased transparency of capabilities, and the interest in collaboratively tracking small vessels through different areas of responsibility hold important implications for future collaborative uses of regional enterprise architectures. On the other hand, the workshop articulated challenges such as the burden of widespread information sharing during daily operations, the need for brokered agreements among diverse stakeholders, and the need for local control of accessibility to shared information.

But MOISA 2 products like the sensor survey and workshops were not just ends in themselves. They also contributed to the articulation and demonstration of a repeatable, evidence-based process for integrating the full range of port partners into the design, development, and fielding of system enhancements to the regional maritime information sharing environment. It is this process that addresses the GAO concern expressed above. It is this process, described primarily in Section 7 but evident throughout this report, which is the primary contribution of MOISA 2.

In the past, federally-led IT projects have generally been managed using a waterfall development process, rather than using more agile, iterative state-of-the-art methods for achieving technology innovation, adoption and sustainable impact. MOISA 2's evolving collaboration with SRI International in support of the DHS S&T IMDE/CSS project has been a unique opportunity to demonstrate the feasibility of applying human centered design and development methods within the context of a federal technology initiative, while articulating the benefits and uncovering key challenges. This approach at the early stage of technology innovation has provided a level of engagement and direction from regional operational professionals that could not have been achieved later in the process. (This integration of regional operators in design activities is still being explored as we continue the partnership with SRI beyond MOISA 2.)

In addition to the impact on design and development, the early and ongoing engagement with a full range of stakeholders also greatly enhances the likelihood of successful transition and sustainability of the IMDE/CSS project should it move into program status. But while these and other benefits of human centered design and development to the IMDE/CSS project are considerable, these benefits are not the primary contribution of MOISA 2. The

benefits of developing and exercising the process itself go beyond any single system or any specific stakeholder, or any particular mission.

In contributing to the IMDE/CSS effort, MOISA 2 developed and exercised a strategic process—a process that is a key component of the overall effort to achieve more successful maritime interagency operations. The co-development of systems invariably surfaces issues such as policy, trust and agency culture that go well beyond the technology itself. By involving diverse maritime stakeholders in an agile, human and mission centered approach to the design and development of their future information sharing environments, we are engaging these stakeholders in dialogs and trust-building partnerships that have real impact, not only on future systems, but in the ways they will collaborate in the future for more efficient and effective mission accomplishment.

This report is one answer to the question of whether or not DHS has a process that will provide "reasonable assurance that [future systems] will satisfy port partners' needs, and facilitate mission-based information sharing to achieve the goals of the IOC project." The answer is yes, and the justification for that assurance is the process presented in this report. And while that process still needs further articulation, exercising, and demonstration, and while there is still a considerable effort needed to move that process into the mainstream of DHS technology innovation, the way forward has begun.

Appendix A: Legal Barriers in Detail

The Wall between Intelligence and Law Enforcement

A national security exemption from the 4th Amendment[137] has been long embraced by the US Government. This exemption, however, has been interpreted to apply only to "pure intelligence" investigations; i.e., the information obtained through warrantless surveillance is inadmissible in prosecution.

Two cases demonstrate the restraint the government has shown in upholding the "pure intelligence" principle. In 1945, the Office of Strategic Services discovered that the Chinese Communism sympathizing magazine, Amerasia, had obtained classified materials from Harry Dexter White, the Assistant Secretary of the Treasury. The evidence of White's espionage, however, had been obtained through warrantless surveillance. No charges were ever brought against White. In another case, Joseph Weinberg, a nuclear physicist who worked on the Manhattan project and who had been bugged by the FBI, was recorded disclosing information to the Soviet Union. Again, the evidence was inadmissible in court, and Weinberg was acquitted.[138]

These and other similar cases illustrated the difference between law enforcement and intelligence investigations. Law enforcement investigation has the ultimate goal of prosecution, and, therefore, 4th Amendment requirements for evidence collection must be kept in mind at all times. Intelligence investigations, on the other hand, may not be related to criminal activity at all, but rather the broader topics of diplomatic, military, and foreign policy. Therefore, two distinct regulatory frameworks have developed; one for domestic law enforcement and one for domestic intelligence activities.[139]

Domestic electronic intelligence surveillance is governed by the Foreign Intelligence Surveillance Act (FISA). FISA allows an agency to surveil a person acting on behalf of a foreign agency without respecting the person's 4th Amendment rights. The information obtained under FISA cannot be used in prosecution. To illustrate the distinction, "FISA electronic surveillance could be conducted primarily to acquire information necessary to recruit a foreign

---

[137] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[138] Atkinson, L.R. (2013). The Fourth Amendment's National Security Exception: Its History and Limits. *Vanderbilt Law Review*, Vol 66, No. 5. pg. 1343-1405.

[139] Ibid.

spy as a double agent, but not to acquire information necessary to prosecute and incarcerate the spy."[140] DEA reinforced "there is a big difference between the Intel world and the real world, going to court world."

Prior to September 11, 2001, investigators working on law enforcement and those working on intelligence did not routinely share information due to constitutional and organizational constraints.[141] The events of 9/11 led Congress to promptly attempt to remove the wall and encourage information sharing between law enforcement and intelligence agencies. Legislative efforts include the USA PATRIOT Act, the Homeland Security Act of 2002 (P.L. 107-296) and the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The Information Sharing Environment (ISE) was created under the Intelligence Reform Act. The ISE is meant to encourage information sharing among federal, state, and local levels of government, including law enforcement and intelligence agencies.[142]

With 9/11 nearly 15 years in the past, Edward Snowden's disclosure of NSA surveillance documents, and the partial sunsetting of the USA PATRIOT Act[143], however, the consensus on removing the wall appears to be reducing.[144]

The Posse Comitatus Act

The Posse Comitatus Act (PCA) of 1878 "restrains the military from making arrests, directly participating in searches and seizures, or directly participating in the gathering of intelligence for [civilian] law enforcement purposes, except when needed for the immediate protection of human life."[145] The Western Air Defense Sector (WADS) reported that the Navy has several sensors that cannot be used/shared: "If a Navy asset tips off a drug bust, it won't stand up in court. It is hard to figure out how we can fit into a proactive force." Another WADS representative went on to state, "We cannot use military assets for civilian law enforcement."

---

[140] Kris, D. S. (2006). The Rise and Fall of the FISA Wall. *Stanford Law \& Policy Review*, Vol 17. pg. 487-488.

[141] Best, R.A. (2007). Sharing Law Enforcement and Intelligence Information: The Congressional Role. A Congressional Research Service (CRS) Report for Congress.

[142] Ibid.

[143] The U.S. government still has significant surveillance authority. Resnikoff, N. (1 June, 2015). ``Sunsetting of Patriot Act will not draw curtain on mass surveillance.'' Al Jazeera America. Retrieved June 7, 2015, from http://america.aljazeera.com/articles/2015/6/1/patriot-act-sunset-leaves-expansive-spying-powers-in-place.html

[144] Best, R.A. (2007). Sharing Law Enforcement and Intelligence Information: The Congressional Role. A Congressional Research Service (CRS) Report for Congress.

[145] Chase, D. W., (22 May 2001). ``Posse Comitatus: A Nineteenth Century Law Worthy of Review For the Future?'', School of Advanced Military Studies, United States Army Command and General Staff College.

Some confusion over when the National Guard is subject to the PCA was evident during the workshops. The National Guard can operate in three different conditions:

1. ***Title 10*** - The United States Code, Title 10 Armed Forces, authorizes the President of the US to order the National Guard to active duty status. Under Title 10, the National Guard is governed by federal policy, federally funded (through the DoD), and subject to Posse Comitatus.

2. ***Title 32*** - The United States Code, Title 32 National Guard, authorizes the state governor to activate National Guard personnel to full-time status. Under Title 32, the National Guard is governed by state policy, federally funded, and NOT subject to Posse Comitatus.

3. ***State Active Duty*** - State governors can activate National Guard personnel to a state active duty status in which personnel become state employees, are governed by state policy, funded by state funds, and NOT subject to Posse Comitatus.

The PCA and Title 10 "govern how and when DoD sensors can be used, and how and when DoD is permitted to share real-time information over communication networks with LEA [law enforcement agency] units, in support of LEA activities."

When a USCG law enforcement officer is on board a US Navy vessel, the USCG law enforcement functions are exempt from Posse Comitatus.

Appendix B: Regional Systems' Modules

Description of Spillman Modules:

Alarm Tracking and Billing module allows users to track false alarms, manage alarm tracking fees, and generate statistical reports, tickets, bills, and correspondence.

Computer Aided Dispatch (CAD) has user-definable features and customizable CAD screens, as well as both mouse and keyboard functionality with keystroke shortcut commands for quickly adding, modifying, assigning, and completing calls. Includes interconnected unit recommendations, mapping and GIS. Provides data field auto population from incoming calls to centralized names, vehicle, property, wanted persons, and law incident tables. Visual and audible alerts provide real-time call updates and critical information such as criminal histories, warrants, wanted persons, and other possible dangers.

CAD Management Dashboard allows personnel to view the number of calls the center receives and track response times. Users can also view incidents on a Google Map™ and customize the dashboard to display specific call natures, date ranges, as well as their agency's name and badge.

CAD Mapping allows the user to view and coordinate the movement of multiple units on a map using visual intelligence about an area, including street names, major buildings, landmarks, service districts, fire/EMS zones, and jurisdictional boundaries. Users can add map layers, customize icons, save specific configurations for later reference, and include an image of a map in a file. Also automatically adds calls to the map as they are received, maps unit locations, and allows users to dispatch via dragging and dropping icons on the map. Hyperlink functionality enables users to link Web cams, traffic cameras, building floor plans, and other

documents or images to a map. CAD Mapping is fully integrated with Spillman's CAD and AVL Mapping modules, GIS functionality, and E-911 Interface.

CAD2CAD Interface allows users to exchange call data with other Spillman and non-Spillman dispatch centers. Provides ability to transfer calls that need to be dispatched by a different agency and communicate live call information when an incident requires a multi-jurisdictional response. Send and receive information such as the location and nature of a call, people involved, and associated vehicles.

Civil Process provides the ability to track each civil process through its lifecycle and print returns for each process. Create a history of attempts, view integrated contact information, manage garnishments, print checks, produce reports, and generate printouts for a variety of civil process costs and services. The Civil Process module also automatically calculates fees and mileage charges, as well as miscellaneous charges, amounts received, and amounts refunded.

Commissary Management provides the ability to manage and record the purchase, sale, and balance of commissary items. View all inmate commissary purchases, account balances, and transaction details, and calculate money owed, balance adjustments, and account closures. The Commissary module also allows users to manage supplier and item data, post and cancel orders, track inventory, set up automatic reorders, print supplier checks, filter items by inmate, and set automatic warnings for inmate restrictions or quantity limits. Bar coding functionality provides commissary item tracking and management.

CompStat Management Dashboard provides crime trend and pattern identification using information in the Spillman database. The dashboard allows you to customize periods of time for which to examine and monitor changes in crime, quality of life factors, and traffic and accident rates.

Crime Monitor, powered by BAIR Analytics, offers integration with an agency's Spillman Records Management System (RMS), providing the ability to share agency-controlled crime data with the public.

E911 Interface provides the ability to receive automatic number and location information (ANI/ALI) from a standard E911 system and transmit the information to the Spillman CAD system. Used in conjunction with the CAD and CAD Mapping modules, the interface enables the user to view real-time locations of both wireless and landline calls on a digital map. Automatic field entry inserts agency-specified information from incoming calls to minimize manual data entry.

Equipment Maintenance allows the user to track the condition, location, history, and upkeep of department equipment, such as ladders, cell phones, shovels, axes, hoses, and saws. Record and schedule maintenance, inspections, repairs, and replacements. Also calculates operating costs and equipment value; tracks warranty, manufacturer, and vendor information; and helps pinpoint causes and determine liability in the event of equipment failure. Integration with CAD and Response Plans modules provides dispatchers with immediate information about equipment availability for emergency responses.

Evidence Barcode & Audit Interface provides bar coding capabilities and a portable handheld bar code reader for evidence room inventory and audit purposes. Automatically transfer scanner data into an evidence record.

Evidence Management allows the user to maintain a complete and accurate chain of custody for every piece of evidence received. The module records changes in an item's location, status, and custodian of evidence, providing a detailed history from the time an agency receives an item until the release or disposal of the item. Full system integration enables the linking of evidence items to name, vehicle, and property information already contained in the database, reducing duplicate data entry. Permit only authorized users to view, add, or modify evidence records.

Integration with the Evidence Bar Code & Audit Interface allows users to label, inventory, and audit evidence items.

Fire Mobile Automatic Vehicle Locator (AVL) Mapping module allows fire personnel to access critical information and view the location of calls and responding units from a single screen. Firefighters can use the module to access information about important on-scene resources as well as data about any hazardous chemicals stored at the site. The Fire Mobile AVL Mapping module also allows firefighters to view call comments and unit statuses of all responding apparatus from the mapping screen.

Fire Mobile CAD module enables firefighters to access mission-critical information while responding to a call. Using the software, firefighters can maintain constant contact with dispatchers and department personnel while freeing up airtime for high-priority calls. Fire Mobile CAD also allows fire personnel to easily view the status of calls and units and quickly access additional call details.

Fire Mobile Premises & HazMat module enables fire personnel to quickly retrieve contact information, floor plans, and the location of alarms. Detailed information about hazardous materials, such as their location and quantity, can also be retrieved while enroute. The module also enables an agency to quickly search and view chemicals in the National Oceanic and Atmospheric Administration (NOAA) CAMEO Chemicals system, which displays full chemical details and helps personnel predict chemical reactivity dangers if specific chemicals are combined.

Emergency Reporting System (EMS) Fire and Emergency Management System Records Interface allows users to complete reports and transfer information from Spillman's CAD module into the ERS fire and EMS reporting and records management system. ERS allows users to manage all fire department's incident reporting, scheduling, training, hydrant maintenance, reports, and personnel requirements from any Internet browser.

Fleet Maintenance provides the ability to regulate and preserve vehicle resources by managing licensing, maintenance, repair, oil service mileage, fuel consumption, registration, inspections, identification, and unit assignment information for fleet vehicles. Provides ability to determine and monitor fleet costs and use historical data to justify future purchasing decisions. Maintenance reminders and reporting also available.

Imaging module provides the ability to capture, import, organize, edit, and share high-quality digital images from an all-in-one application. The module also allows users to automatically generate appropriate lineups as well as capture and edit images to meet National Institute of Standards and Technology (NIST) standards.

Insight uses a multi-system, multi-jurisdictional data sharing broker to run real-time queries on the databases of other participating agencies for names, associated images, vehicles, property information, and other records, regardless of whether they are using Spillman or a non-Spillman information database. InSight enables simultaneous, multi-agency returns from one search and incorporates the Global Justice XML Data Model (GJXDM) as well as advanced data encryption and user-defined privileges. Searches can be conducted from a PC or via a Web-based browser on a laptop or mobile device.

Inventory Management tracks supplier and ordering information and automatically updates balances and reorder points. Pre-formatted reports for purchase orders.

Jail Management records booking procedures, inmate tracking, risk and medical assessment, and reporting. Includes a step-by-step booking checklist. Assessments are customizable and decision tree-based. Complete integration with the Law Records module to obtain stored name information and see how an inmate is connected to incidents, property, aliases, and more. Other detailed tables allow users to track and view all medical information, flags and warnings, cash accounts, and scheduled events.

Law Records with UCR/MIBRS tracks a variety of information for both criminal and non-criminal incidents, including complainants, victims, offenders, suspects, witnesses, evidence, vandalism, arson, vehicles, and stolen and recovered property. Complete integration with Spillman's CAD module automatically copies pertinent call information into related records, and information can be accessed in real time anywhere in the system. Detailed crime summary and activity information such as offenses, arrests, and law incidents for submitting UCR and NIBRS reports electronically to state and federal agencies can be compiled. Other features include case management and automatic visual alerts.

Licenses & Permits allows users to manage animal and bicycle licenses, weapon and fire permits, and other types of licenses and permits. Detailed information can be entered and tracked, including expiration dates, fees, payments, and adjustments. The module also allows the printing of permits, receipts, mailing labels, and reports. Immediate access to other Spillman modules and tables, such as the property table, allows for efficient search capabilities.

Mobile AVL Mapping technology allows users to track the location of all fleet units in real time through Global Positioning System (GPS) receivers. View the location of nearby units to determine where the closest officer is for backup, or view CAD calls on a jurisdictional map. The Quickest Route feature improves response times by dispatching the unit closest to a call by analyzing actual drive time, your local street network, and barriers such as rivers, canyons, and limited-access highways. Integration with Google Earth™ allows users to replay, review, and evaluate vehicle routes. CAD Mapping automatically adds and updates calls to the map as they come in.

Mobile Driver License Scanning modules allows scanning of a driver license and automatically populates Mobile search screens with the driver's name, date of birth, address, physical description, and a driver license identification number. A scan instantly queries the local database as well as state and National Crime Information Center (NCIC) databases. Data

gathered from a driver license is also available to quickly pre-fill and complete field reports. The module is compatible with both bar-coded and magnetic stripe driver licenses.

Mobile Accident Forms allows users to record accident data and complete accident forms from user's vehicle. Large fields and drop-down menus are easy to navigate using either a touch-screen monitor or a keyboard and mouse. Forms can be customized with agency's name, graphics, and a report title. Use prefilled form data to complete fields with information from driver license scans or previous name and vehicle queries. Forms attach to Spillman records for viewing, editing, and printing, and the system automatically searches for matching records before storing the information and routing electronically for approval. Add an unlimited number of people, vehicles, property, associated details, and narratives, and add custom fields. The Mobile Accident Forms are ideal for agencies that do not need a state-specific solution.

Mobile Citation Forms provides ability to issue traffic and municipal citations from user's vehicle. Large fields and drop-down menus are easy to navigate using either a touch-screen monitor or a keyboard and mouse. Forms can be customized with agency's name, graphics, and a report title. Use prefilled form data to complete fields with information from driver license scans or previous name and vehicle queries. Forms attach to Spillman records for viewing, editing, and printing, and the system automatically searches for matching records before storing the information and routing electronically for approval. Add an unlimited number of people, vehicles, property, associated details, and narratives, and add custom fields. The Mobile Citation Forms are ideal for agencies that do not need a state-specific solution.

Mobile Law & Field Interview Forms allows user to conduct field interviews and record data from a vehicle. Large fields and drop-down menus are easy to navigate using either a touch-screen monitor or a keyboard and mouse. Forms can be customized with agency's name, graphics, and a report title. Save time and prevent mistakes using drop-down lists of prefilled data wherever possible. Forms attach to Spillman records for viewing, editing, and printing, and they system automatically searches for matching records before storing the information and

routing electronically for approval. Add an unlimited number of people, vehicles, property, associated details, and narratives, and add your own custom fields.

Mobile Premises & Hazmat provides field access to data on the location, type, and container size of hazardous materials stored in a designated jurisdiction as well as detailed premises information such as number of floors, responsible agencies, and physical descriptions. The National Oceanic and Atmospheric Administration (NOAA) CAMEO database offers information on more than 4,000 chemicals, including recommended handling instructions, first-aid responses, and protective clothing. Proximate population information helps to organize warnings and evacuations.

Mobile Records provides the ability to instantly access system data from the field without leaving the vehicle and without dispatcher assistance. A single query allows a search of the local database, other Spillman and non-Spillman databases, and state and national databases. In addition to searching names, vehicles, incidents, property, and wanted persons, users are able to search more than 20 other types of system records.

Mobile State & National Queries uses a state connection to search state and national databases for name, vehicle, property, guns, and wanted person records as well as available images. State and federal searches can be performed simultaneously with one query while using the local RMS query feature to search local database information. Returns are delivered audibly as well as with visual highlights, including any alerts on records containing warnings.

Mobile State eCitation Form modules allows the creation and completion of traffic citation forms electronically. Users can search Name, Vehicle, and Property records in Spillman Mobile and transfer information from search results to the electronic form using drag-and-drop mouse actions or keyboard commands.

Mobile Voiceless CAD module allows field personnel to access real-time call information from their laptop computers. The module also enables personnel to quickly update their status, add and view call comments, and efficiently access radio logs and incident information.

Pawned Property provides the ability to record pawnshop activities to assist in locating stolen property. Designed to accommodate the laws and procedures of any state or county, this module will help track and record pawnshop visits, spot checks, hits, and recovery of stolen items. Preformatted reports identify individuals with frequent activity and determine recovery rates. Integration throughout the Spillman system provides a cross-reference to the names, law incident, and property tables for details.

Personnel Management allows secure access to key information on each of an agency's employees, including special skills, medical history, training and certifications, positions held, attendance, activities, leave time, and overtime. Accounting of administrative activities such as commendations and disciplinary actions is also provided. Integration with the CAD module gives dispatchers access to personnel expertise, while ensuring the privacy of each employee with file security features. Attendance and workload management tools help you monitor employee availability and productivity.

Pin Mapping provides plotting of jurisdictional crime data on a pin map. Visual displays are customizable and can be saved for later use, and viewing options include orthographic, street, fire, and water layers. A comprehensive toolbar allows users to adjust map layers, colors, and incidents shown. Distance measuring tools help to identify related crimes and suspects.

Premises & HazMat Information provides the recording of extensive data on residential, commercial, or public lots within a jurisdiction and respond appropriately to disasters or calls at unfamiliar sites. The National Oceanic and Atmospheric Administration (NOAA) CAMEO database offers information on more than 4,000 chemicals, including recommended handling instructions, first-aid responses, and protective clothing. Proximate population information

helps to organize warnings and evacuations. Integration with Spillman's GIS and CAD verifies an address as a call is entered and indicates whether premises information exists for that location.

Response Plans allow users to define the agencies and units that will respond to a law, fire, or EMS call at each specified alarm level. A resource list provides an instant view of all available resources within an agency or a neighboring agency. Integration with Spillman's Personnel, Equipment, and Premises & HazMat modules available. When used with the Fire Records module, user can also access hydrant and water source information.

Rip and Run module allows information about a call to be sent directly from Spillman's CAD module to the fire department, providing firefighters with a printout to take with them as they respond to the call. Reports can also be sent electronically to e-mail addresses or other destinations, depending on agency's software configuration.

Sex Offender Tracking module gives agencies the ability to enter, manage, and track critical data on sex offenders and meet requirements for the Sex Offenders Registration and Notification Act (SORNA). Agencies using the module can connect a sex offender alert with any name record, which can then be seen on associated vehicle and address records in the Spillman system. Personnel can assign, schedule, and record tasks like officer calls and visits, as well as track the registration information and status of a sex offender. The module also gives agencies the ability to monitor the distance a sex offender lives or works from vulnerable locations.

Spillman Analytics module offers agencies a map-based analytics tool to assist in Intelligence-Led Policing (ILP) initiatives, helping them make informed decisions about their resources. With multiple data layers and customizable time and date ranges, agencies can use many tools to analyze data, including crime-specific filters, heat maps, pin maps, time comparison analytics, and more. Spillman Analytics gives users the ability to create geographic profiles for

quick access to specific areas for hotspot monitoring. Users can also create up to 20 customized dashboards to view and analyze data.

Spillman Touch module allows public safety personnel to access records and images, search for data, view dispatch information, and receive call assignments using a mobile device. Full integration with agency's Spillman database enables user to see dispatch calls as they are received and update unit's status. Users can search for name, vehicle, property, and incident records and see related alerts and warnings in situations where desktop or laptop computers aren't accessible.

StateLink gives the ability to access information about wanted persons, warrants, stolen vehicles, missing persons, criminal histories, vehicle registrations, driver license information, and other critical data with a single query into state, national, and other external databases. Queries are sent securely and can be accessed from the StateLink request screen, from the CAD module, from a record in any Spillman module, or from a list of recent transactions. Agencies can set security privileges to allow only authorized user access. Query or transaction can be submitted from both desktop PCs and mobile units, and responses can be printed or e-mailed. Transaction logs automatically record all queries, ensuring system security. The Mobile Office: State & National Queries module offers additional features for personnel submitting queries from the field.

Traffic Information provides the ability to track, reference, and record accident, citation, and warning data to make informed decisions about traffic conditions and trends in a jurisdiction. Fields defined for citations, road and weather conditions, offense codes, and accident severity promote proper data entry. Complete Spillman system integration automatically records information from the Traffic Information module into related name and vehicle records already in the system. When used with Spillman's Imaging module, users can also attach multiple high-quality digital images of vehicles and accident scenes to records.

Vehicle Impound allows users to keep accurate, detailed records of all vehicles that are impounded, released from impound, or sold. Record information for the vehicle, owner, driver, towing company, status, location, impound circumstances, sale, and price. Fee management tools help to organize impound, towing, and storage fees, and preformatted notifications make it easy to notify interested parties of intent to sell. Record single or batch sales and automatically stop the calculation of storage charges for sold vehicles.

Description of Washington Common Operation Platform Component Applications:

Adashi is a response and command software tool that integrates with CAD to provide GPS navigation, routing and communication, along with geographic information.

Mutualink is an interoperable communications and media sharing solution.

Wrike is an online task and project management platform to help stakeholders manage day-to-day and emergency tasks, projects or incidents.

IWSAlerts is an emergency Mass Notification System (EMNS) and Crisis Communication application.

Sahana is a solution to manage organizations, people, projects, inventory and assets in large-scale emergencies and disasters.

Appendix C: Operational Planning & Scheduling Preliminary Interview Protocol

INTRO

Explain why we are here: Our work is sponsored by DHS S&T, the DHS Interagency Operations Centers program (IOC) led by Coast Guard HQ, the National Maritime Intelligence-Integration Office (NMIO) and the Program Manager for the Information Sharing Environment (PM-ISE). DHS S&T has funded the development of an enterprise architecture called the Integrated Maritime Domain Enterprise (IMDE) intended to deliver interoperability in support of regional security and safety operations. Puget Sound is one of the demonstration sites, with a technical demonstration currently scheduled for November 2015 and an operational demonstration scheduled for March 2016. Before this system comes to the region, we would like to understand what you do and how you do it and how a system like IMDE might impact your work. This is an opportunity for you to influence the design and development of IMDE as it will appear in our region.

This 30 minute, semi-structured interview will focus on how you plan and manage your activities and assets. Following this session, we will need to schedule a one-hour session with the current version of IMDE, built around a planning and management use case. When are you available?

Time follow up session scheduled: _____

The test will require you to use your work computer to access our test version of the software via the Web. Who is the IT POC at your organization who we can contact to ensure that this is possible?

Name and contact info for IT POC: _____

Later this summer, after we've given the results to the IMDE project, there will likely be a chance to test how well they have addressed the user group's input. The goal is to help DHS close the gap between what they currently have and what the regional community wants.

INTERVIEW

Focus on scenario: Again, our objective is to understand how you plan and schedule the allocation and deployment of resources to carry out day-to-day security operations (e.g., patrol). Do you have any questions?

How do you plan and schedule the allocation and deployment of resources to carry out day-to-day security operations? (Day in the life)

What triggers your planning?

Who or what else is involved before, during, after?

What are the main steps?

What information do you need and how do you get it?

Please show us examples

Do you have any MOUs or Information Sharing Agreements that impact this work?

What are the pain points? How could it be done better?

What should I have asked you that I didn't?

Appendix D: CSS-IMDE Planning and Scheduling

User Test Documentation

Contents:

1. Pre-test (15 minutes)
    a. Introduction (3 minutes)
    b. Administrator set up (2 minutes)
    c. Over-the-shoulder training (10 minutes)
2. Exercise (20 minutes)
    a. Test script and task descriptions
3. Post-test (25 minutes)
    a. System Usability Scale (SUS) – (5 minutes)
    b. Satisfaction questionnaire - (5 minutes)
    c. Closing questions - (15 minutes)
4. Administrator documents
    a. Instructions for reset dashboard
    b. Form for recording observations
    c. Show card for Likert scale Qs

PRE TEST MATERIALS

INTRODUCTION (3 minutes)

Hello [Participant's Name],

Thanks for taking the time to meet with me. Please make yourself comfortable.

Throughout our meeting I'll be referring back to this script just to make sure that I don't forget anything.

As you know, our work is sponsored by DHS S&T, the DHS Interagency Operations Centers program (IOC) led by Coast Guard HQ, the National Maritime Intelligence-Integration Office (NMIO) and the Program Manager for the Information Sharing Environment (PM-ISE). DHS S&T has funded the development of an enterprise architecture called the Integrated Maritime Domain Enterprise (IMDE) intended to deliver interoperability in support of regional security and safety operations. Puget Sound is one of the demonstration sites, with a technical demonstration currently scheduled for November 2015 and an operational demonstration scheduled for March 2016. This is an opportunity for you to influence the design and development of IMDE as it will appear in our region.

This is not a product test. This is an exercise of an in-development system. By participating in this session you are part of the design team. The purpose of this exercise if for you to help us understand how a system like this might impact your work and to improve its design.

This session includes a brief training on how to use the software demo followed by two exercises in which you will interact with the demo around a planning and scheduling use case. We will run through the use case twice. The first time I will give you some guidance, breaking it down into tasks; the second time, I will let you drive the activity. We will close with some questions about your experience. The entire session should take about an hour.

This is not an evaluation of your performance. I will provide you training on everything you need to know how to do in the software demo, and if you need me to remind you how to do something, please ask. Your answers to the closing questions are confidential. You have the right to refuse to answer any question at any time with no penalty to you.

Some of the potential long-term benefits to you for participating in this exercise include improvements to your organization's work processes. The benefit to society is that your participation can help us better understand how to develop tools to help you do your job and ultimately help improve regional safety and security.

Throughout the exercise, we will be using a think aloud protocol. This means that I would like you to say whatever you are thinking, doing, or looking at as we proceed. The purpose of this is for me to try and understand the tacit knowledge that you bring to this work. I may probe for more information or to ask additional questions. If you have any questions for me, please don't hesitate to ask. If you need a break, please feel free to speak up.

So that I don't miss anything, I would like to capture a screen and audio recording of our session. Is that all right with you? I will also be taking notes.

Do you have any questions?

<Answer any questions>

Thank you. Now we will begin.

SET UP THE CREEN RECORDING

1. Open quick time
2. Select "New screen recording" from file menu
3. Ensure that built in microphone is selected in drop down menu that appears on recording box.

LOG IN TO DEMO

1. In Google chrome, go to: https:97.76.231.109/owf

OVER THE SHOULDER TRAINING MATERIAL

- **First I would like to introduce you to the different UI elements we see.**
  - Planning
    - This is the planning widget. Up above you have the resources view that lets you see the supply of assets by agency (scroll to the agency we are at)
    - When you click on split screen, you also get the mission view, which let/s you see the missions that are scheduled for a given day and the number of requested resources that have been assigned to the mission so far.
  - User directory
    - This is the user directory. It allows you to view other users of the app and their contact info. It also allows you to contact them via send a message.
  - Map
    - This is the map. It allows you to view and adjust the positions of missions and assets
  - UI Interactions
    - To change the size of any windows, click and drag on the black bar between panes. This has been a bit glitch in the past.
- **UI details**
  - Planning
    - The upper half of the split screen is the resources view. This To see the resource details, single click on a resource (this takes a while to populate)
      - In resource details, you can assign a person to a resource using the dropdown & link at the top
      - Notice that there are two tabs—one for planning (today) and another for tomorrow planning. Later on, I will ask you to complete a task that requires you to look at activities planned to occur "tomorrow," and you can get to tomorrow's plan by clicking on the tomorrow planning tab.

To look at missions scheduled for a given day, click on the Split button

- The time grid shows when the mission is scheduled to take place.
- The numbers are how many resources are assigned, how many are needed.

- To see the resources attached to a mission, click the down arrow
- To assign a resource to a mission, then drag a resource onto a mission in the time during which that mission is scheduled to occur. Right now, it is not possible to unassign a mission.
- The resource will appear as a yellow blob on the map at Victoria, but we will go over the map widget in a moment.
- Only one of the missions in the scheduling grid can be open at any time. so opening a second one automatically closes the first one.
- Once a resource is assigned, it will vanish from the resource panel while the mission is open—this is to prevent you from assigning the same resource to the same mission twice.
- To see that the resource has been assigned to the mission, close the mission in the mission pane and the mission shows in the resource pane in the planning view.
- To see mission details, single click on the mission. This opens the mission details properties sheet. You can also get here in full screen mode by clocking on a mission in the schedule.

Mission Details

In mission details, you can see what resources have been assigned.
The "add" and "remove" buttons don't currently work.

User Directory

To chat with someone in the directory, click "Send Message"
To search for users, you can sort the entries.

Map

Resources appear as yellow blobs; missions appear as life preservers. In this version, the only mission that will appear on the map is the "Operation Seagull" that we will work through in this case. To move resources around on the map, click and drag them
As I mentioned, when you add a new resource, its default location is Victoria
If you add more than one resource, they will stack up at Victoria until their location is adjusted, so if you don't see a newly added resource appear right away, it might be hiding behind another one.
To find out more information about resources on the map, hover your mouse over it.
If you want more information on a mission on the map, you can click on it.

That is all for the training overview. Again, if you forget how to do something, just ask, and I will remind you.

Do you have any questions right now?

Just give me a moment to reset the dashboard prior to beginning the exercise.

<ADMINISTRATOR RESETS DASHOBOARD>

EXCERCISE MATERIALS

Task #	Task description - Prompt given by administrator // Administrator prompt for user-reported task completion criteria	What the user sees	Actions* *Required actions in black; *possible subsequent actions in gray*		Questions this task will help us answer
1	*Your first task is to review your current schedule.* Tell me when you are clear on what is happening today	Dashboard shows planning widget (split screen view) in upper right, user directory widget in lower right, and map on the left. Planning shows data for today.	• Scroll to own agency in resources pane	•	• Does the application present information in a way that enables users to gain situational awareness of their own agency's daily operations?
N/A	*Introduce trigger:* **Background** – You receive a phone call requesting support for an event due to occur tomorrow. This event is the movement of the M/V Polar Pioneer Mobile Offshore Drilling Unit, The Polar Pioneer, which is currently anchored at Terminal 3, Everett, will begin transit toward Alaska. The Polar Pioneer will transit under tow and will have a 500 yard safety zone around it and a 100 yard safety zone while moored at Terminal 3. Current planning for tomorrow is available in the CSS-IMDE application. This event has been given the name "Operation Seagull." **Activity** – The activity is to use CSS-IMDE to obtain additional information about the event, to determine how you will respond to the request, including how you might plan and schedule any resources' you decide to allocate in support of this event, in the context of your current schedule. Your goals are to both (a) respond to requests for your resources to support the event and (b) make any necessary adjustments to your current schedule.				
2	Familiarize yourself with the plan and schedule for date of the event. Tell me when you know enough about the current plan to begin planning how you might assist.	Planning widget shows resource and mission schedules for day of the event.	• Navigate to "tomorrow planning" • *Scroll through agencies in resources pane* • *Click on "Operation Seagull" in mission pane to open mission details* • *Click on Operation Seagull in resource pane to see resources assigned*	•	• Does the application present information in a way that enables users to understand plans for an interagency operation

			• *View planned location of assets on map*		
3	Determine which, if any, of your assets you can commit to supporting Operation Seagull Tell me what you decide about committing assets to the event	• Own agency's asset list in planning pane • *Resource details* • *Mission details*	• Scroll to your own agency in resources pane • *Open resource details* • *Open staffing from drop-down list to assign staff to resource* • *Open mission details* • *View mission map* • *Toggle between full and split screen in planning widget* • *Open user directory to send a message to others*	•	• Does a system like this support decision making around operational planning and scheduling? • Does a system like this support user in identifying how their resources might be used to best support a collaborative operation? • Does a system like this enable users to consider the plans and schedules of other agencies in their own planning? • Does a system like this support users in weighing trade-offs associated with having a limited number of resources to meet a greater number of mission possibilities? • Does a system like this support communication required to coordinate collaborative missions?
4	Assign any assets you can allocate in support of the event to the mission Tell me when you have assigned all the assets you wish to allocate to the mission	• In the resource view the asset is scheduled to "Operation Seagull" • "Mission details" now lists new asset in resource list • New asset appears on mission map	• Open split screen view • Open black triangle under "Operation Seagull" • Drag and drop the asset to mission "Operation Seagull" in mission area of planning widget (split screen)	•	• Does the "drag and drop" interaction fit with users' mental model of resource assignment? • Does a system like this give users adequate feedback as to whether their resources have been assigned to the correct mission?
5	For any assets to be assigned, indicate the desired starting location for the mission Tell me when you have the asset(s) to their	• Asset moves on map in response to click and drag	• Click and drag asset to desired starting location	•	• Does a system like this support users' decisions about where to position their resources geographically in order to best support a collaborative operation?

	planned starting location(s)				• Does a system like this support users' understanding of how their decisions regarding planning and scheduling will impact other agencies/operations that are nearby?
6	Now that we have run through this scenario and you understand the demo, let's return to the beginning, to where you get the call about the event. Now show or tell me what you would really do? Feel free to use the demo or whatever other tools you need to support your explanation. TEST ADMIN – REFRESH BROWSER	Varies	Varies		• How would users use or not use a system like this to support their decision making around planning and scheduling their resources?
7	Show me how you would review the impact of this change on your daily operational schedule	Varies	Varies		• Does a system like this support users ' understanding of the impact of schedule changes on daily operations?
8	Show me how you would adjust your daily operational schedule to minimize the impact of event participation on daily ops.	Varies	Varies		

POST-TEST MATERIALS

Participant name, agency: _____ Test Date: _____

DEBRIEFING PROTOCOL

We will now go through a set of structured questions followed by a few open-ended questions about your experience. For the structured questions, we will use the Likert scale on the show card I provided. You will answer with how you feel in response to a statement on a scale of 1-5; 1, strongly disagree and 5 is strongly agree. There is also an N/A option for questions where you feel you don't have enough information to answer. For these structured questions, I don't want you to deliberate for too long—I want you to go with your gut, or your initial reaction.

Throughout the questionnaire, you will ask you how you feel about "this version of the system" or "a system like this." By "this version" and "like this" I mean a system with the same system concept and design, but one that is fully functional rather this limited demo in which much of the actual functionality has yet to be built out.

SYSTEM USABILITY SCALE (SUS)

	Strongly disagree 1	2	3	4	Strongly agree 5	N/A
1. I think that I would like to use a system like this frequently						
2. I found this version of the system unnecessarily complex						
3. I thought this version of system was easy to use						
4. I think that I would need the support of a technical person to be able to use a system like this						
5. I found the various functions in this version of system were well integrated						
6. I thought there was too much inconsistency in this version of the system						
7. I would imagine that most people would learn to use a system like this very quickly						
8. I found this version of the system very cumbersome to use						
9. I felt very confident using this version of the system						
10. I needed to learn a lot of things before I could get going with this version of the system						

Participant name, agency: _____ Test Date: _____

SATISFACTION, INFORMATION SHARING AND SAFEGUARDING,

	Strongly disagree 1	2	3	4	Strongly agree 5	N/A
1. Overall, I am satisfied with this version of the system						
2. I would recommend a system like this to a friend						
3. This system works the way I want it to work						
4. I feel I need to have a system like this						
5. A system like this is secure in handling sensitive information.						
6. Overall, a system like this is trustworthy.						
7. Agencies that partner with my own will have concerns about security, privacy, and confidentiality associated with a system like this.						
8. In general, I believe that partner agencies will be satisfied with a system like this.						
9. A system like this will contribute to my agency's ability to collaborate with partner agencies for improved mission accomplishment.						
10. A system like this would allow me to work with an appropriate level of sensitivity to others' need for information sharing and safeguarding.						
11. If I had access to a system like this at work, I would use it.						
12. If a system like this were available, it would be helpful for my agency and agency partners.						

Participant name, agency: _____ Test Date: _____

CLOSING QUESTIONS

1. What, in general, would you use a system like this for?

2. Do you feel that a system like this has the potential to improve your current planning and scheduling process? If so, how? If not, why?

3. What did you like about using this version of the system?

4. What was difficult or challenging about using this version of the system?

5. What information do you feel you needed but did not have? For any information that you felt was missing, where do you currently get this information?

6. If there were one or two things you would change about this version of the system, what would they be?

ADMINISTRATOR MATERIALS

TEST OBSERVATION CODING FORM

DATE: _____ PARTICIPANT: _____TASK #: _____

START TIME: _____ END TIME: _____

Verbal Behaviors	**Notes**
☐☐☐☐ Strongly positive comment	_____
☐☐☐☐ Other positive comment	_____
☐☐☐☐ Strongly negative comment	_____
☐☐☐☐ Other negative comment	_____
☐☐☐☐ Suggestion for improvement	_____
☐☐☐☐ Question	_____
☐☐☐☐ Variation from expectation	_____
☐☐☐☐ Stated confusion	_____
☐☐☐☐ Stated frustration	_____

Non-verbal behaviors	**Notes**
☐☐☐☐ Laughing/happy	_____
☐☐☐☐ Surprised	_____
☐☐☐☐ Variation from expectation	_____
☐☐☐☐ Random mouse movement	_____
☐☐☐☐ Groaning/deep sigh	_____

Task completion status

Incomplete (1)
- ☐ Participant gave up
- ☐ Task "called" by moderator
- ☐ User believed complete, but not

Partially complete (.5)
- ☐ Complete with assistance
- ☐ Moderator restated task
- ☐ Moderator navigated back to starting dashboard

Complete (0)
- ☐ Fully complete

SHOW CARD

TRIGGER FOR EXERCISE

Background – You receive a phone call requesting support for an event due to occur tomorrow. This event is the movement of the M/V Polar Pioneer Mobile Offshore Drilling Unit, The Polar Pioneer, which is currently anchored at Terminal 3, Everett, will begin transit toward Alaska. The Polar Pioneer will transit under tow and will have a 500 yard safety zone around it and a 100 yard safety zone while moored at Terminal 3. Current planning for tomorrow is available in the CSS-IMDE application. This event has been given the name "Operation Seagull."

Activity – The activity is to use CSS-IMDE to obtain additional information about the event, to determine how you will respond to the request, including how you might plan and schedule any resources' you decide to allocate in support of this event, in the context of your current schedule. Your goals are to both (a) respond to requests for your resources to support the event and (b) make any necessary adjustments to your current schedule.

5-POINT SCALE FOR QUESTIONNAIRE

Strongly disagree				**Strongly agree**	
1	2	3	4	5	N/A

Appendix E: Repeatable Mechanisms

Table A: List of Surveys/RFI/Reports reviewed		
Title	**Sponsor/Author(s)**	**Interviewees**
Port interagency information sharing (2008-2009 report)	USCG Information Sharing Executive Agent	USCG sectors and sector-identified FSLTIPP partners
IOC Watchkeeper Survey	IOC Program Office, USCG Office of Shore Forces	IOC users Watchkeeper
Ad hoc customer service and information quality survey	United States Coast Guard	IOC employees who use Watchkeeper
Maritime Information Sharing Taskforce (MIST) Report	Naval Postgraduate School & Federal and Commercial Stakeholders	IOC employees
Seattle Sensor Survey Report	IOC, USCG	
Assessment of the WatchKeeper Technology Demonstrator	IOC	Operational WatchKeeper account holders
Request for Information (RFI) Data Call	National Security Council Staff (NSCS)	One respondent per agency
Data Tagging Survey	The Information Integration Subcommittee (IISC) of the Information Sharing and Access Interagency Policy Committee (ISA IPC)	Offices or individuals who focus on enterprise data management and/or enterprise architecture for completion (27 respondents)
Key Information Sharing and Safeguarding Indicator (KISSI) worksheets		Operators
2014 Performance Assessment Questionnaire (PAQ) Response Aggregation	Frank Sisto frank.sisto@navy.mil Sean Tweed-Kent stweed@nmic.navy.mil Archana Vuyyuru archanav@dni.gov	
Interoperability Maturity Model & Assessment Table Top Exercise Check List		

Table B: Semi-structured interview protocol for interviews with surveyors and survey respondents		
Q #	**Who**	**Question**
1	Surveyor, Participant	What is your role in the survey process? Creator, Sender, Responder, Analyzer?
2	Surveyor, Participant	If there were one thing you could change about the survey process, what would it be?
3	Surveyor, Participant	Can we get a sample of past surveys you have created or received?
4	Surveyor, Participant	Are you interested in seeing results of past surveys or knowing what surveys were done in the past? If so, what information are you interested in having from a survey? In what format would you like to have this information?
5	Participant, Surveyor	How many requests to participate in/are you involved in per year?
6	Participant	In an average year, how many do you get that should have been sent to someone else?
7	Participant	What influences your decision of whether to participate in a voluntary survey?
8	Participant	How much does whom the survey or RFI comes from influence your decision to participate?
9	Participant	How would you prefer to be approached about completing a survey?
10	Participant, Surveyor	What is your process for completing/creating/distributing a survey? How did you come up with this process (was it something you were taught? Came up with on your own…?)
11	Participant	Do you need approval to complete a survey? If yes, who is the approver? What is the process for getting approval?
12	Surveyor	How do you know whom to solicit for survey responses? Is this part of the formal process?
13	Surveyor	What tools are available to assist with the survey creation process? Do you use these tools? Why or why not?
14	Surveyor	Have you come up with any techniques for improving your response rate (i.e., what do you do to ensure highest possible response rate?)

Table C: List of interviewees		
#	**Name**	**Agency/Organization**
1	Marvin Ferriera	APM Terminal Tacoma
2	Tim Lupher	USCG
3	Scott Pollack	MEXPS
4	Margaret Schwertner	Consultant, Moffatt & Nichol
5	Stephanie Supko	County Emergency Management
6	Sean Tweed-Kent	NMIO
7	John Ventjeer	MEXPS

Appendix F: Statement of Work Reference Matrix

		Assigned Tasks:							
		4.1.1	**4.1.2**	**4.1.3**	**4.2.1**	**4.2.2**	**4.2.3**	**4.2.4**	**4.2.5**
Chapter 1	Executive Summary	X							
Chapter 2	Introduction	X							
Chapter 3	Background	X	X						
Chapter 4	Sensors and Sensor Opportunities		X		X	X			
Chapter 5	Technology Analysis: IMDE/CSS and Related Regional Systems in Use		X					X	
Chapter 6	Use Cases		X	X			X		
Chapter 7	MOISA's Role in IMDE Development			X			X		
Chapter 8	Repeatable Mechanisms			X					X
Chapter 9	Discussion and Conclusions	X							
Appendix A	Legal Barriers in Detail			X	X				
Appendix B	Regional Systems' Modules							X	
Appendix C	Operational Planning & Scheduling Preliminary Interview Protocol			X			X		
Appendix D	CSS-IMDE Planning and Scheduling			X			X		
Appendix E	Repeatable Mechanisms			X					
Appendix G	CUI Guide			X					

Appendix G: CUI Guide

The Center for Collaborative Systems for Security, Safety, and Regional Resilience

AT THE UNIVERSITY OF WASHINGTON

Information Security Guide

August 15, 2015

CENTER FOR COLLABORATIVE SYSTEMS FOR SECURITY, SAFETY & REGIONAL RESILIENCE

UNIVERSITY of WASHINGTON

Controlled Unclassified Information (CUI) Guidance

Issued and Approved by:

_____

Dr. Mark Haselkorn, PhD. Director of CoSSaR

_____

Date

Table 1: Version Control		
Version	**Change**	**Effective Date**
Version 1.0	Initial Version	

Table 2: Table of Changes				
Version #	Date	Section	Paragraph	Description

Table of Contents

List of Tables

1 GENERAL

1.1 PURPOSE

This Information Security Guide is issued for the purpose of identifying specific topics of information associated with projects under the Center for Collaborative, Safety, Security, and Regional Resilience (CoSSaR) that meet the standards and criteria for special handling and protection in accordance with Executive Order 13556, "Controlled Unclassified Information" (CUI). The document also provides guidance on handling sensitive information that requires protection against unauthorized disclosure, including information designated "Sensitive But Unclassified" (SBU) under current control programs, which will ultimately be transitioned to protect information under the new CUI regime.

This guide provides direction for identifying and properly handling the three categories of CUI/SBU information most likely to be encountered by the CoSSaR community:

- "For Official Use Only" (FOUO) (See Section 5)
- "Law Enforcement Sensitive" (LES) (See Section 6)
- "Sensitive Security Information" (SSI) (See Section 7)

All CoSSaR project information designated or determined to be CUI/SBU must be processed according to the requirements of this Information Security Guide. However, the vast majority of the information gathered, processed, analyzed, and produced in CoSSaR activities will be "Unclassified" information without the need for special handling. Unclassified information which is not designated CUI/SBU by the originator ***and*** which does not meet the criteria for CUI/SBU set forth in this Information Security Guide and reference documents in Section 1.2 does not require special handling or safeguarding.

This guide does not address national security classified information deemed Confidential, Secret, or Top Secret as set forth in Executive Order 13526.

1.2 AUTHORITY

This guide is approved by the Director of the Center for Collaborative, Safety, Security, and Regional Resilience at the University of Washington. It is issued to provide guidance to Federally directed CoSSaR activities in accordance with Executive Order 13556, Department of Homeland Security Management Directive Numbers 11042.1 and 11056.1, Department of Defense Manual Number 5200.01 (Volume 4), 49 CFR 1520.5, and University of Washington security directives.

1.3 SCOPE AND APPLICABILITY

This document provides security guidance for the use of CUI/SBU information associated with the CoSSaR program. This guide and reference authorities (listed in Section 1.2) shall be cited as the basis for recognizing, categorizing, marking, handling, processing, transmitting, and disseminating of CUI/SBU and materials. If a conflict exists between this guide and reference authorities, the reference authority takes precedence.

1.4 EFFECTIVE DATE AND IMPLEMENTATION

This guide is effective immediately upon release.

1.5 OFFICE OF PRIMARY RESPONSIBILITY

The Office of Primary Responsibility (OPR) for this guide is:

Program Manager
Center for Collaborative, Safety, Security, and Regional Resilience (CoSSaR)
310 Sieg Hall, Box 352315
University of Washington
Seattle, WA 98195
Phone: (206) 543-4640 Fax: (206) 543-8858 E-Mail: CoSSaR@uw.edu

The office of secondary responsibility for this guide is:

University Facility Security Officer
1013 NE 40th St., Box 355640
Seattle, WA 98105
Phone: (206) 543-1315 Fax: (206) 543-1732 E-Mail: uwfso@uw.edu

2 POLICY

2.1 GENERAL

One goal of CoSSaR is to produce relevant analytic products for Puget Sound area stakeholders that may be disseminated to the widest audience possible at the uncontrolled UNCLASSIFIED level. In the conduct of their work, CoSSaR researchers may, however, be given CUI/SBU information - or they may create it by compilation. To properly control information, it is essential for researchers to recognize CUI/SBU information.

When gathering information, it is ***required*** that CoSSaR researchers document when the information they receive is CUI/SBU information. All information marked as CUI/SBU by any Federal agency shall be marked and handled in accordance with this Information Security Guide within the CoSSaR project. It is the responsibility of each CoSSaR researcher to ask if information gathered in verbal interviews is either uncontrolled or CUI/SBU information.

Department of Homeland Security (DHS) Management Directive 11042.1 states "Any DHS employee, detailee, or contractor, can mark information falling within one or more of the categories as FOUO." Therefore, acting as grantees or contractors to DHS, CoSSaR researchers may designate information falling into the categories below as "FOUO" to maintain protection of the information. Additionally, "DHS Officials occupying supervisory or managerial positions are authorized to designate other information, not listed and originating under their jurisdiction, as FOUO."

If CoSSaR personnel believe that information meets the criteria for CUI/SBU information, the material should be sent to the sponsor team via DHS using approved CUI/SBU information transmission methods (see section 4.3) for final determination. In the interim, the material shall be protected as if it were CUI/SBU information until a final determination is made by DHS.

2.2 REASON FOR CONTROL

Most unclassified information encountered and produced during the conduct of research under the CoSSaR project will not be subject to special controls. However, certain categories of unclassified information are exempt from public release under the Federal Freedom of Information Act, the Privacy Act, and the US Code of Federal Regulations (CFR). This information is designated CUI/SBU information, and must be protected from unauthorized public release. (For more information on the details of the regulatory authority, see Sections 5, 6, and 7).

2.3 CONTROL BY COMPILATION

Analysis and compilation of uncontrolled unclassified information is normally not subject to the restrictions associated with CUI/SBU information. However, in certain circumstances, information that would otherwise be uncontrolled may become CUI/SBU information when combined or associated with other unclassified information, if the compiled information reveals an additional association or relationship, not otherwise evident by the individual items of information that meets the standard and criteria for CUI/SBU information. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is CUI/SBU, not the individual items of information.

3 RELEASE OF INFORMATION

3.1 PUBLIC RELEASE

This guide is designated UNCLASSIFIED and subject to public release under the Federal Freedom of Information Act and Washington RCW Chapter 42.56 Public Records Act.

3.2 CONTROLLED UNCLASSIFIED INFORMATION

Executive Order 13556 "Controlled Unclassified Information" established the CUI program, which is a system that standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. Although President Obama signed Executive Order 13556 in 2009, many Federal agencies have yet to complete the transition to the CUI standard. As a result, much of the guidance for the previous "Sensitive But Unclassified" (SBU) regime remains in place.

This guide applies to certain types of CUI/SBU information for which Executive Branch agencies require applications of controls and protective measures for a variety of reasons. FOUO and LES are designations applied by DHS to CUI/SBU information, which may be exempt from mandatory release to the public under Section 552 of Title 5, U.S.C., "Freedom of Information Act (FOIA)" or "The Privacy Act". SSI is the designation applied by DHS to CUI/SBU information obtained or developed in the conduct of security activities as defined in 49 C.F.R. Section 1520.5.

4 INFORMATION HANDLING

4.1 GENERAL HANDLING REQUIREMENTS

1. No security clearance is needed for access to CUI/SBU information; however, the recipient must have a 'need to know' the information.

2. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. CUI/SBU information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the materials shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items. CUI/SBU information should not be stored with classified information unless there is a correlation.

a. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal CUI/SBU information to unauthorized persons, a "FOR OFFICIAL USE ONLY" or "Sensitive Security Information" cover sheet will be used to prevent unauthorized or inadvertent disclosure. (For further information on cover sheets see Sections 4.2.2, 4.2.3, and 4.2.4.)

b. When forwarding CUI/SBU information, a FOUO or SSI cover sheet should be placed on top of the transmittal letter, memorandum, or document.

3. Unauthorized disclosure of CUI/SBU information doesn't constitute a security violation, but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of CUI/SBU information protected by the Privacy Act may result in criminal sanctions.

4. To obtain further guidance regarding For Official Use Only (FOUO) and Law Enforcement Sensitive (LES) refer to DHS Management Directive Number 11042.1.

5. To obtain further guidance regarding the handling of Sensitive Security Information (SSI) refer to DHS Management Directive Number 11056.1.

4.2 DOCUMENT MARKING

4.2.1 UNCLASSIFIED (U)

Unclassified refers to information that requires no security protection and can be released to individuals without restrictions. To identify unclassified information in a title, heading, paragraph, or bullet, precede it with a portion marking (abbreviated classifications listed before each paragraph) of "(U)". If a document contains uncontrolled unclassified material only, annotate "UNCLASSIFIED" in the header and footer, or do not place any classification markings on the document.

4.2.2 FOR OFFICIAL USE ONLY (FOUO)

To identify unclassified information, designate it with an "FOUO" caveat in a title, heading, paragraph, or bullet, precede the portion with "(U//FOUO)". If a document contains both "(U)" and "(U//FOUO)", the overall classification of the document is "UNCLASSIFIED//FOR OFFICIAL USE ONLY," as annotated in the header and footer.

Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. At a minimum, prominently mark on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information may be further marked with an applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE", in order to alert the reader of the type of information conveyed. (See Section 4.2.3.) Additional access and dissemination restrictions may also be cited as the situation warrants.

The cover sheet of each document containing FOUO should be marked with the following warning:

(U) WARNING: This document is UNCLASSIFIED // FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or

other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

4.2.3 LAW ENFORCEMENT SENSITIVE (LES)

In unclassified documents containing LES information, the phrase "Law Enforcement Sensitive" shall accompany the phrase "FOR OFFICIAL USE ONLY" at the bottom of the outside of the front cover, the title page (if there is one), and the outside of the back cover (if there is one). Each page containing FOUO-LES information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" at the bottom.

Portions of unclassified documents that contain FOUO-LES information shall be marked with the parenthetical notation "(FOUO-LES)" at the beginning of the portion. If an unclassified portion of a classified document contains FOUO-LES information, the portion marking (U//FOUO-LES) shall be used.

The cover sheet of each document containing LES should be marked with the following warning:

(U) WARNING: LAW ENFORCEMENT SENSITIVE. The information in this document marked FOUO-LES is the property of the Department of Homeland Security and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior DHS authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.

4.2.4 SENSITIVE SECURITY INFORMATION (SSI)

To identify unclassified information with an "SSI" caveat in a title, heading, paragraph, or bullet, precede the portion with "(U//SSI)". If a document contains "(U)", "U//FOUO", "(U//LES)", and "(U//SSI)", the overall classification of the document is "UNCLASSIFIED// LAW ENFORCEMENT SENSITIVE and SENSITIVE SECURITY INFORMATION".

Individual paragraphs and sections properly marked as "Unclassified" or "(U)" may be shared freely, but other information properly marked as FOUO, LES, or SSI within a document can only be shared with authorized recipients who have a valid "need-to-know".

The cover sheet of each document containing SSI should be marked with the following warning:

> *(U) WARNING: This record contains SENSITIVE SECURITY INFORMATION that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.*

4.2.5 ORIGINATION INFORMATION

Designator or originator information & markings, downgrading instructions, & date/event markings are not required on FOUO, LES, or SSI documents.

4.2.6 REMOVAL OF CUI MARKINGS AND DESIGNATION

Removal of CUI/SBU information markings can only be accomplished by the originator or other competent authority. ***DO NOT*** remove any CUI/SBU information markings

without written authorization from DHS, NAVSEA Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I), or the originator.

4.3 TRANSMISSION OF CUI/SBU INFORMATION

4.3.1 MAIL

Controlled Unclassified Information may be mailed via First Class Mail with the U.S. Postal Service, or an authorized commercial delivery service such as DHL or Federal Express.

a. SSI shall be mailed in a manner that offers reasonable protection of the sent materials and sealed in such a manner as to prevent inadvertent opening and show evidence of tampering.

b. SSI may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access (e.g., sealed envelope).

4.3.2 VOICE, DATA, AND FAX

Electronic transmission of CUI/SBU information (voice, data, or facsimile) should be by approved secure communications systems *whenever practical*.

a. Unless otherwise restricted by the originator, CUI/SBU information may be sent via non-secure fax. Where a non-secure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

4.3.3 ENCRYPTION

CUI/SBU information transmitted over email should be protected by encryption, such as the use of password protected files. When encryption is impractical or unavailable transmit over regular email channels.

4.3.4 UNENCRYPTED FILES

Unencrypted files containing CUI/SBU information shall ***NEVER*** be stored or transmitted using commercial file sharing systems (e.g., Dropbox).

4.3.5 PUBLIC WEBSITES

CUI/SBU information should not be posted to public websites.

a. SSI may be posted on approved government-controlled or –sponsored encrypted or otherwise protected portals, such as the Homeland Security Information Network (HSIN), USCG HomePort, or TSA's WebBoards. Such posting shall be in accordance with guidance published or approved by the TSA SSI Office and appropriate IT security offices.

4.4 RELEASE TO ELIGIBLE STAKEHOLDERS

CoSSaR may disseminate CUI/SBU information to its employees and subcontractors who have a need for the information to complete work assigned in connection with CoSSaR projects.

CoSSaR seeks to provide its CUI/SBU information-designated analytic products the widest distribution among Puget Sound area stakeholders with a legitimate "need to know".

a. The CoSSaR Program Manager will seek permission from its DHS sponsor team to release reports containing CUI/SBU information to each individual stakeholder requesting the information.

b. The CoSSaR Project Manager will also comply with University procedures for the release of CUI/SBU information by submitting a University Access Request Form to release CUI/SBU information to regional stakeholders.

C. The CoSSaR Project Manager will maintain a log recording the release of all CoSSaR products and reports containing CUI/SBU information to third parties.

4.5 DESTRUCTION

Hard copy CUI/SBU materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

Electronic storage media shall be sanitized appropriately by overwriting or degaussing. After destruction, materials may be disposed of with normal waste.

Paper products containing CUI/SBU materials will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

4.6 INCIDENT REPORTING

The loss, compromise, suspected compromise, or unauthorized disclosure of CUI/SBU information will be reported to the CoSSaR program's DHS sponsor team and the University of Washington Office of Sponsored Programs within one business day of the discovery of the incident.

Incidents on UW IT systems will also be reported to the University Facility Security Officer at 206-543-1315 or uwfso@uw.edu via the system's Information Technology Manager (http://ciso.washington.edu/report/). Coordinate reporting through the HCDE IT Manager for incidents on the HCDE server or the APL IT Manager for incidents on APL-hosted servers.

Suspicious or inappropriate requests for CUI/SBU information by any means (e.g., email or verbally) shall be reported to the DHS sponsor team via the CoSSaR Program Manager and the UW Office of Sponsored Programs.

If the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned ongoing operation, additional notifications to appropriate DHS management personnel will be made without delay.

In the event of an unauthorized disclosure, CoSSaR will request an inquiry by the University Facility Security Officer to determine the cause and effect of the incident and suggested corrective actions to prevent recurrence.

5 General Guidance, "FOR OFFICIAL USE ONLY"

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as "For Official Use Only". ***This is an abridged list*** containing the most likely topics CoSSaR researchers are expected to encounter in the conduct of their research. ***Appendix A contains a list of all topics provided by DHS in Management Directive 11042.1.***

Table 3: FOUO General Guidance		
For Official Use Only – 5 USC 552 (FOIA and Privacy Act)		
Topic	**Marking**	**Remarks**
FOIA (5 USC 552) Exemption 1: Properly classified information	As Marked	CoSSaR will not receive, process, or handle classified material.
FOIA (5 USC 552) Exemption 2: Records related to the internal personnel rules and practices of an agency.	FOUO	
FOIA (5 USC 552) Exemption 3: Information that has been specifically exempted from disclosure by statute.	FOUO	
FOIA (5 USC 552) Exemption 4: Trade Secrets (narrowly defined)	FOUO	
FOIA (5 USC 552) Exemption 5: Inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.	FOUO	
FOIA (5 USC 552) Exemption 6: Personnel, medical, and similar files	FOUO	

FOIA (5 USC 552) Exemption 7: Law enforcement information	FOUO-LES	See Law Enforcement Sensitive Matrix for further guidance
FOIA (5 USC 552) Exemption 8: Matters/information for regulators or supervisors of financial institutions	FOUO	
FOIA (5 USC 552) Exemption 9: Geological information and data, including maps, concerning wells	FOUO	
Privacy Act (5 USC 552a) § (j)(2): Material reporting investigative efforts pertaining to the enforcement of criminal law, including efforts to prevent, control, or reduce crime or to apprehend criminals.	FOUO-LES	See Law Enforcement Sensitive Matrix for further guidance
International and domestic information protected by treaty, statute, regulation, or other agreement.	FOUO	
Information that could result in physical risk to personnel.	FOUO	
System security data revealing the security posture of a system.	FOUO	For example: threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, etc…
Information that reveals security vulnerabilities, whether to persons, systems, or facilities.	SSI	See Sensitive Security Information Matrix for further guidance

6 General Guidance, "Law Enforcement Sensitive"

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as "Law Enforcement Sensitive". The list contains abridged descriptions. Appendix B contains the full descriptions of Law Enforcement Sensitive exclusions to the FOIA as delineated by the US Department of Justice.

Table 4: LES General Guidance		
Law Enforcement Sensitive – Exemption 7 of FOIA (5 USC 552)		
Topic	**Marking**	**Remarks**
Information that could reasonably be expected to interfere with enforcement proceedings	FOUO-LES	
Information that would deprive a person of a right to a fair trial or an impartial adjudication	FOUO-LES	
Information that could reasonably be expected to constitute an unwarranted invasion of personal privacy	FOUO-LES	
Information that could reasonably be expected to disclose the identity of a confidential source	FOUO-LES	Including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation,

		information furnished by a confidential source
Information that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law	FOUO-LES	
Information that could reasonably be expected to endanger the life or physical safety of any individual	FOUO-LES	

7 General Guidance, "Sensitive Security Information"

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as "Sensitive Security Information" as delineated in 49 US Code of Federal Regulations (CFR) §1520.5.
(From https://www.tsa.gov/sites/default/files/assets/pdf/ssi/16_categories_ssi.pdf)
(See also: https://www.law.cornell.edu/cfr/text/49/1520.5)

Table 5: SSI General Guidance		
Sensitive Security Information – 49 CFR (Code of Federal Regulations) §1520.5		
Topic	**Marking**	**Remarks**
Security Programs and Contingency Plans	SSI	Includes amendments, comments, guidance regarding: i. Domestic aircraft operator, airport, foreign a/c, FBO, or IAC security program or contingency plan ii. Vessel, maritime facility, port security plan [maritime only] iii. National or area security plan [maritime only] iv. Security incident response plan [maritime only]
Security Directives (SDs) or orders	SSI	i. Issued by TSA for domestic aircraft or airport operators ii. Issued by Coast Guard [maritime only] iii. Related comments, guidance
Info Circulars or notices issued by DHS or DOT regarding aviation or maritime threats	SSI	i. Info Circulars (ICs) issued by TSA ii. Navigation or Vessel Inspection

		Circulars (NAVICs) issued by USCG [maritime only]
Performance specifications, test objects, and test procedures	SSI	i. Detection devices used by Fed Government for aviation or maritime security [devices] ii. Security communications equipment used for aviation or maritime [comm. equipment only]
Vulnerability assessments directed, created, held, funded, approved by, or provided to, DOT or DHS	SSI	
Security Inspection or investigation information	SSI	i. Details revealing an aviation or maritime vulnerability (less than one year old), including airport and aircraft name and violation description; identity of investigating Federal employee ii. (After one year) specific gate or airport location; (within one year) airport violation summaries [release airport and a/c name and violation description after one year]
Threat information against transportation held by Government	SSI	

Security measures: specific details of aviation or maritime security measures	SSI	i. Measures recommended by the Government ii. Procedures and #s of Federal Air Marshals (FAMs) or USCG security personnel iii. Procedures, or aggregated #s by aircraft operator, of Federal Flight Deck Officers (FFDOs) iv. Armed security officer procedures [Armed Security Officer Prog. for DCA general aviation]
Security screening info (aviation or maritime)	SSI	i. Procedures, incl. comments, guidance, and selection criteria, for screening persons, carry-on or checked baggage, U.S. mail, and stores [CAPPS criteria] ii. Info and sources of info of screening systems [actual No Fly lists] iii. Detailed locations of particular screening methods or equipment [requires determination] iv. Any security screener tests and scores [written, procedural, computer-based tests] v. Performance or testing data from security equip. or screening systems [operational tests] vi. Any electronic image on

		screening equip. monitors, incl. TIPS images/descriptions
Security training materials created for aviation or maritime security training purposes	SSI	
Identifying info of certain transportation security personnel	SSI	i. Lists of names or identifying info: [lists, not individual names] 1. Having unescorted access to secure area of airport or maritime facility 2. Security screeners aggregated by airport 3. USCG personnel conducting vulnerability assessments, security boardings, other operations 4. FAMS ii. FFDOs [individual names, not just lists]
Critical aviation or maritime infrastructure asset info	SSI	i. Prepared by DHS or DOT ii. Prepared by State or Local government and submitted to DHS or DOT
Confidential business information related to aviation or maritime security	SSI	i. Solicited or unsolicited proposals ii. Trade secret info obtained by DHS and DOT iii. Commercial or financial info, if not otherwise customarily disclosed

Research and Development info	SSI	Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.
Other	SSI	Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

APPENDIX A: Information Controlled as "For Official Use Only"

1. Information that is exempt from release under FOIA (5 U.S.C. 552)
http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-exemptions.pdf

a. Exemption 1: Protects properly classified information.

b. Exemption 2: Protects records that are "related solely to the internal personnel rules and practices of an agency."

c. Exemption 3: Protects information that has been "specifically exempted from disclosure by statute."

d. Exemption 4: Protects trade secrets (narrowly defined).

e. Exemption 5: Protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."

f. Exemption 6: Protects information in personnel and medical files and similar files when disclosure would constitute a clearly unwarranted invasion of personal privacy.

g. Exemption 7: Protects six different types of law enforcement information: On-going proceedings; Personal Privacy; Confidential sources; Techniques and procedures. (See Law Enforcement Sensitive section below).

h. Exemption 8: Protects matters contained in or related to examination, operating, or condition reports prepared by or for regulators or supervisors of financial institutions.

i. Exemption 9: Protects geological information and data, including maps, concerning wells.

2. Information that is exempt from release under Privacy Act (5 U.S.C. 552a)
http://www.fbi.gov/foia/privacy-exemptions

a. Information compiled in reasonable anticipation of a civil action proceeding.

b. Material reporting investigative efforts pertaining to the enforcement of criminal law, including efforts to prevent, control, or reduce crime or to apprehend criminals.

c. Information that is currently and properly classified pursuant to an executive order in the interest of the national defense or foreign policy—for example, information involving intelligence sources or methods.

d. Investigative material compiled for law enforcement purposes, other than criminal, which did not result in the loss of a right, benefit, or privilege under federal programs or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence.

e. Material maintained in connection with providing protective services to the U.S. President or any other individual pursuant to the authority of Title 18, U. S. Code, Section 3056.

f. Required by statute to be maintained and used solely as statistical records.

g. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence.

h. Testing or examination material used to determine individual qualifications for appointment or promotion in federal government service—the release of which would compromise the testing or examination process.

i. Material used to determine the potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

3. Information within the international and domestic banking and financial communities protected by statute, treaty or law.

4. Other international and domestic information protected by treaty, statute, regulation, or other agreement.

5. Information that could be sold for profit.

6. Information that could result in physical risk to personnel.

7. DHS Information Technology (IT) internal systems data.

8. System security data revealing the security posture of a system. For example threat assessments, system security plans, risk management plans, etc…

9. Information that reveals security vulnerabilities, whether to persons, systems, or facilities.

10. Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten national security.

11. Overly revealing information of developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

APPENDIX B: Law Enforcement Sensitive (LES) Information

http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7_0.pdf

Exemption 7 of the Freedom of Information Act protects from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information that

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual."

DEFINITIONS

Access. The ability and opportunity to obtain knowledge of classified information.

Classified National Security Information. Information that has been determined pursuant to E.O. 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also, known as classified information.

Compilation. An aggregation of pre-existing unclassified items of information. Compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification pursuant to E.O. 13526 and is not otherwise revealed by the individual information. Classification by compilation must meet the same standards and criteria as other original classification actions.

Document. Recorded information regardless of the nature of the medium or the method or circumstances of recording.

For Official Use Only (FOUO). The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interests. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 13526, "Classified National Security Information", or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by produced by or for, or is under the control of the United States Government.

Law Enforcement Sensitive (LES). "Law Enforcement Sensitive" is a marking sometimes applied, in addition to the marking "FOR OFFICIAL USE ONLY," by the Department of Justice and other activities in the law enforcement community, including those within the Department of Defense. It denotes that the information was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests.

Lawful Request. Any formal request for information or records that is made under the auspices of existing statute or regulation, for example, information or records requested under the Freedom of Information Act (FOIA).

Need-to-know. A determination within the executive branch in accordance with directives issued pursuant to E.O. 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Sensitive Security Information (SSI). As defined in 49 C.F.R. Section 1520.5, information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would (1) constitute an unwarranted invasion of privacy (including , but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

Unclassified. Information not meeting criteria for classification set forth in Executive Order 13526.