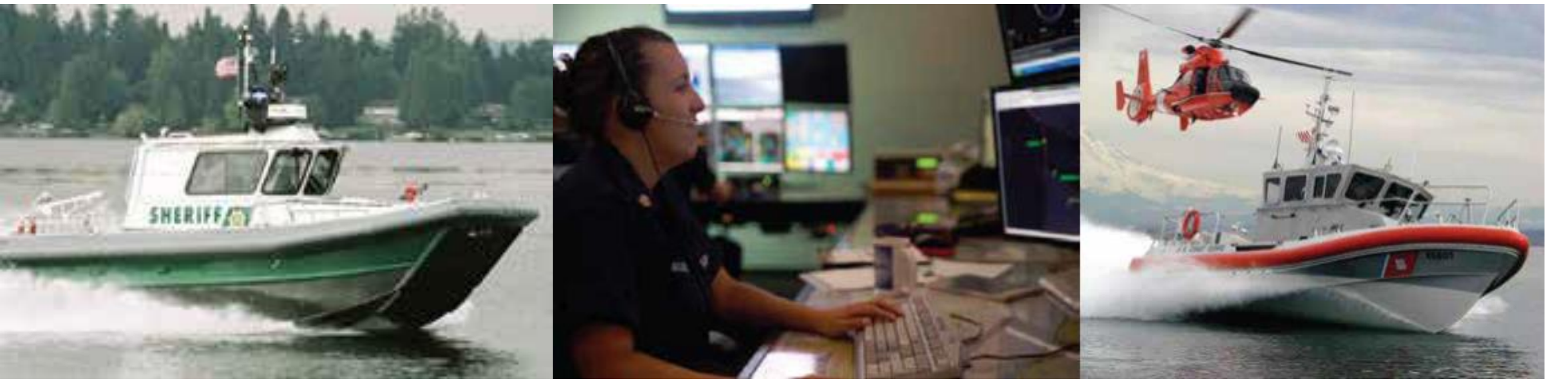


Project Interoperability in Puget Sound:

A Regional Mission-Centric Perspective on Information Sharing and Safeguarding

October 2016

Version 2.00

Prepared by the Center for Collaborative Systems for Security, Safety and Regional
Resilience
at the University of Washington

Prepared for the Program Manager for the Information Sharing Environment
the Department of Homeland Security S&T First Responders Group,
the Department of Homeland Security Interagency Operations Center, and
the National Maritime Intelligence-Integration Office

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

First printing, September 2016

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/

Acknowledgements

The University of Washington acknowledges the contributions made to the research and publication of the Project Interoperability in Puget Sound Report. We are especially grateful to the Puget Sound safety and security operational community, both for what they do every day, and for their generous participation without which this research would not have been possible.

We would also like to thank the sponsors for their financial and in-kind support and contributions as partners in this project, in particular:

- Ken "Doc" Holliday for the Program Manager for the Information Sharing Environment
- Paul Reisner for the Department of Homeland Security Science & Technology First Responders Group
- Brad Clark and Mark Miller for the Department of Homeland Security Interagency Operation Center
- Chris Hickey for the National Maritime Intelligence-Integration Office

Research Team

Faculty: Mark Haselkorn, Mark Zachry
Research Scientists: Keith Butler, Sonia Savelli, Brian Zito
Staff: Chris Hussein, Sarah Yancey
Graduate Research Assistants: Melissa Braxton, Chris Lewis, Maureen Rowell, Brett Fuller, Nick Zimmer
Liaison: Anne Tyler

Table of Contents

Acknowledgements iii

Table of Contents iv

List of Tables vi

List of Figures vii

1 Executive Summary 1

2 Introduction and Overview 3

3 Project Interoperability 9

3.1 Analysis of Project Interoperability Tools 11

3.1.1 Interoperability Tools for Management and Administration 12

3.1.2 Interoperability Tools for Infrastructure Integration 14

3.1.3 Interoperability Tools for the Standards Community 14

3.1.4 Interoperability Tools for Data Exchange 15

3.2 Towards Community-based, Mission-centric Project Interoperability Tools 23

3.2.1 The Information Sharing Matrix 24

4 Use Cases 27

4.1 Use Case One: Planning and Scheduling Capabilities 27

4.1.1 As-is Process Analysis 28

4.1.2 Mission-based Opportunities for Interoperability 34

4.1.3 Conclusion 35

4.2 Use Case Two: Resource Requesting and Tracking Post-Disaster 36

4.2.1 Emergent Events Overview 36

4.2.2 Interoperability Tools and Concepts 38

4.2.3 Tool Usefulness 45

4.2.4 Considerations for a Future Network of Interoperable Systems 49

4.3 Overview Across the Two Use Cases 49

5 Community Information Sharing and Safeguarding 51

5.1 Qualitative Analysis of Interoperability 51

5.1.1 Interagency Collaboration 53

5.1.2 State-level Disaster Management 55

5.2 Qualitative Study Conclusions 57

6 A Plan of Action for Moving Forward 58

List of Tables

Table 1: Resources Used by Selected Regional Agencies 28

Table 2: Functional Areas of Interoperability in Scheduling and Planning 33

Table 3: Access Control Systems Used....................43

Table 4: Identity Management Systems Used....................43

Table 5: NIEM and Related Standards Used....................44

Table 6: Policy Constraints Towards Interoperability 44

Table 7: Interoperability Tool Improvement Challenges 54

List of Figures

Figure 1: The Interoperability Continuum (From Interoperability, SCC Whitepaper, v.1, 12 October 2015) 12

Figure 2: Breakdown of PI tools (Ten PI Tools in Black Font) 13

Figure 3: Project Interoperability Tools and Concepts 24

Figure 4: Example of Matrix Showing Information Sharing Relationships 25

Figure 5: Lummi Nation PD Sender Worksheet 26

Figure 6: Content Analysis Summary for Planning and Scheduling Use Case 53

Figure 7: Content Analysis Summary for Resource Request and Tracking Use Case 55

1 Executive Summary

Project Interoperability in Puget Sound (PIPS) took the perspective of operational stakeholders working on a daily basis to maintain regional security and public safety. From this perspective, we found considerable evidence that federally sponsored interoperability initiatives need to shift focus from "bottom up" machine and data standards to "top down" issues of mission, policy, law and organization. This is not to say that bottom up standards efforts are not important and necessary; rather that once the top-down issues are addressed and the regional community has taken ownership of an interoperability innovation, articulated what they want and how they are willing to work collaboratively to make it happen, then the machine and data standards become vital tools for making it happen. But without solving the complex higher level issues first, the lower level standards will sit there like hammers looking for a nail.

PIPS proposes moving forward on three fronts:

1. Shifting Project Interoperability (PI) and other federally sponsored interoperability initiatives higher up the "interoperability continuum," that is, towards community partnerships that co-develop and demonstrate mission-based tools and concepts.
2. Establishing model regional resource centers that address stakeholder needs regarding achieving mission benefits through interoperability innovation and enhanced information sharing.
3. Incorporating state-of-the-art human centered design and development strategies and methodologies into interoperability initiatives. These design and development strategies and methodologies foster innovations that are co-created, mission-centric, agile, iterative and that integrate issues of motivation, policy, law and workflow throughout the project.

PIPS reviewed existing PI tool initiatives and found that outside of Federal agencies (and often even within those), these interoperability tools and concepts are currently having little impact on the regional Information Sharing Environment (ISE) of State, local or tribal security and safety agencies. The PI tools were broken down into five categories: (1) tools for management and administration, (2) tools for infrastructure integration, (3) tools for standards developers, (4) tools for data exchange to manage identity and access, and (5) tools for data exchange to facilitate coordinated operations. None of these categories went beyond machine and data to include policy, legal, organizational and other non-technical issues. PI initiatives require an expansion of scope that includes partnering with operational agencies to identify and add tools that are community-based and mission-focused. We provided an example of such a tool for trust-based interoperability.

We did in-depth analysis of two use cases: (1) planning and scheduling of daily operations and (2) resource requests and tracking during emergent events in the Puget Sound region. These cases revealed the great diversity of the regional ISE and the challenges to interoperability, especially the critical importance of those challenges that go beyond machines, networks and data. They also revealed the effectiveness of the existing, less formal, more flexible ISE which is based primarily on trust, relationships and shared experiences. Additional analysis of the qualitative data obtained from these cases further demonstrated the lack of impact of existing PI tools and confirmed that the current PI tool set should include tools to address the mission-oriented interoperability layer.

This report concludes with a POAM that includes seven project activities through which CoSSaR will partner with regional operational stakeholders, Federal interoperability leaders, and interoperability experts and researchers from academia and industry to move national interoperability efforts towards more mission-based, community-centered design, development, implementation and evolution. As documented in this report, this movement is crucial for the success of our nation's program to promote innovation aimed at achieving appropriate and effective information sharing and safeguarding.

PIPS was sponsored by the Program Manager for the Information Sharing Environment (PM-ISE) and the Department of Homeland Security (DHS), and supported by the DHS/U.S. Coast Guard Interagency Operations Center (IOC) and the National Maritime Intelligence-Integration Office (NMIO). PIPS was conducted by the Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR) at the University of Washington.

2 Introduction and Overview

There are numerous government agencies and industry consortia working in various environments on projects aimed at achieving enhanced interoperability. These projects all face numerous challenges, but the most fundamental of these challenges is that there is not yet a clear shared understanding of what it means to improve interoperability. Some efforts rely on definitions that focus on machines and data, such as:

> *Interoperability describes the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user.*[1]

This type of definition views interoperability as a shared state of technical systems and devices that enables them to exchange understandable data. Other efforts put collaborative goals at the center of interoperability. The European Interoperability Framework, for example, views interoperability in terms of public service.

> *Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.*[2]

This type of definition views interoperability as a collaborative state of organizations and people sharing information in service of a common mission. Tensions can arise between efforts based on improving interoperability as a more machine-and-data-centric, standards-based activity versus those based on a view of interoperability as a more mission-centric, distributed understanding across people and organizations linked by a shared operational mission.

In March 2014 at the annual WIS3 Conference in Reston Virginia, Project Interoperability (PI) was launched as a partnership between the Federal Government, spearheaded by the Office of the Program Manager for the Information Sharing Environment (PM-ISE), and the Standards Coordinating Council (SCC), an advisory group of standards organizations and industry consortia. From its initiation, PI encompassed the many facets and definitions of "interoperability."

[1] *What is Interoperability?* The Healthcare Information and Management Systems Society (HIMSS), http://www.himss.org/library/interoperability-standards/what-is-interoperability

[2] *European Interoperability Framework*, European Commission, 2010. http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

With an advisory body led by standards organizations, it is not surprising that machine-and-data-centric perspectives and issues were well represented. PI was described as a "start-up guide" providing "tools and resources… in different levels of maturity" with "the content of Project Interoperability com[ing] directly from the I^{2}F"—the ISE Information Interoperability Framework. I^{2}F is described as "a framework from which concrete reference architectures and implementations are used to share or exchange information."[3] This focus on technology frameworks aligned with the stated goal of PI "to help government and non-government organizations identify a baseline of terms, tools, and techniques to connect networks and systems."[4]

To further a technology framework for enhanced interoperability, PI presented ten "tools for building information interoperability." These tools are listed below in an order that we established, to match the categorization presented in section 3.1 where the tools are analyzed.

Springboard: This is an evaluation and certification program designed to help industry and government programs ensure compliance [sic] with information sharing standards.

Maturity Model. This is an approach for describing the various stages of implementation of any system or program. The five stages, in order from least mature to most mature, are: ad hoc, repeatable, enhanced, managed, and optimized.

Architecture Alignment. This refers to the process required to create interoperability between different architectures. For example, an architecture alignment would be required for a DoDAF system to "talk to" a TOGAF system.

Reference Architecture Template. This is a data-agnostic template for an architecture, which provides a common vocabulary for implementation.

Common Profile. This describes high-level details associated with any program or system (such as the interoperability profile or metadata).

[3] *ISE Informationn Interoperability Framework (I^{2}F)*, Version 0.5, March 2014, p. ix.

[4] https://github.com/Project-Interoperability/project-interoperability.github.io/blob/master/README.md, Accessed 08/30/2016. [NOTE: As of the writing of this report, all PI websites were in DRAFT form and still under construction.]

ISE Standards Specifications Framework. This describes interoperable information exchange attributes beginning with standardized requirements and definitions. It includes the descriptive mechanics to develop components and processes necessary to identify and normalize standards to achieve interoperability.

Identity and Access Management. This is a diverse portfolio of services and processes that provides identity management, authentication, and authorization.

Attribute Exchange. This is the ability of two or more organizations to make access-control-related information on its users available to each other programmatically and on demand.

Exchange Patterns. This provides generic solutions to help demonstrate a commonly occurring need for exchange of data or information between two or more partners.

National Information Exchange Model (NIEM). This is a sector-based, standards-driven approach to exchanging data.

These "Interoperability Tools" operate largely within the machine-and-data-centric perspectives of interoperability (see analysis below in Section 3.1).

In addition to perspectives that focus on standards for machines and data, PI also addressed the perspective of interoperability as a collaborative state of organizations exchanging information in service of a shared mission. PM-ISE collaborates actively with operational agencies like the Coast Guard and works to highlight "the shared role by federal, state, local, tribal, and territorial (FSLTT) ISE stakeholders."[5] Thus while I^{2}F took its definitions of interoperability from more technical, machine-centric bodies such as the IEEE,[6] PI incorporated mission into many of its definitions, such as its definition of "information interoperability" where even "a technical perspective" includes mission.

> *Information interoperability is the ability to transfer and use information in a consistent, efficient way across multiple organizations and IT systems to accomplish operational*

[5] *ISE Annual Report to the Congress*, August 2016, p. 1.

[6] For example, "Information interoperability is defined in this document as 'the ability to transfer and use information in a uniform and efficient manner across multiple organizations and information technology systems.' It is the ability of two or more systems or components to exchange information and to use the information that has been exchanged." from *ISE Information Interoperability Framework (I^{2}F)*, Version 0.5, March 2014, p. vii.

> *missions. From a technical perspective, interoperability is developed through the consistent application of design principles and design standards to address a specific mission problem.*[7]

Project Interoperability in Puget Sound (PIPS) was born out of a perceived need to better understand this mission-centric, distributed stakeholder side of PI; to find out what impact, if any, the more standards-based PI tools were having on the regional operational communities; and to recommend how to best move forward to improve interoperability at the regional operational level. Thus PIPS began with three overarching questions:

(1) How useful and applicable to mission accomplishment are the interoperability tools and concepts?

(2) Why may some tools not be useful?

(3) What strategies can be used to improve tool design, usability, and outreach?

The goal was to answer these questions and develop a plan for moving forward towards improved interoperability from the perspective of the diverse operational community of regional information sharing stakeholders.

In achieving this goal, PIPS built upon a previous partnership among PM-ISE, the U.S. Coast Guard Interagency Operations Centers Program (IOC), the National Maritime Intelligence-Integration Office (NMIO), and the University of Washington's Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR), called the Maritime Operations Information Sharing Analysis (MOISA). In the two years prior to PIPS, MOISA built on existing relationships among the Puget Sound security and safety community to analyze and understand the regional information sharing environment (ISE). Rather than focus on emergency response and management, MOISA focused on the business-as-usual interagency information sharing processes, data, technology, and communication systems that support day-to-day maritime operations.

MOISA found that daily operational information sharing among the diverse set of regional agencies and stakeholders relied more on informal systems based on relationships and trust, using ubiquitous "technologies" like email, phone and meetings, rather than relying on formal agency-specific computer systems with secure logons based on standards of identity and access management. This is not to say that regional agencies

[7] http://project-interoperability.github.io/, Accessed 08/30/2016.

are not using computational information systems and digital databases to accomplish their work, but rather that they are not using these largely disconnected systems to create and implement an information sharing community. Given this, it is not surprising that PIPS found little direct impact of the formal PI tools on current regional interoperability mechanisms that support what is largely an informal information sharing environment.

Since MOISA focused on daily operations, PIPS included an analysis of interoperability during disaster response and management operations. This enabled us to study and compare interoperability during both business-as-usual and disaster response incident command situations. The two PIPS "use cases" selected for in-depth analysis were: (1) the planning and scheduling of an interagency operation to provide a security zone around a towed vessel, and (2) the requesting and tracking of assets following a major regional disaster. Fortuitously, PIPS coincided with the largest regional disaster response exercise ever conducted in the Northwest – Cascadia Rising. This multi-state, international response to a massive Cascadia subduction zone scenario became the focal point for our second use case as well as an opportunity for additional analysis of interoperability issues for a county Emergency Operations Center (EOC) engaged in disaster response.

From these two use cases and other analyses, PIPS learned that during both business-as-usual and disaster scenarios, from the perspective of the regional operational community, interoperability is a mission-focused means rather than an infrastructure-focused end. For regional agencies, a completely interoperable infrastructure that does not provide tangible operational enhancements to mission accomplishment is like a new highway or beautifully paved road that does not take them directly to where they need to go. There are always costs to the regional agencies to travel on this new highway, and to date the benefits of travel have not outweighed those costs. (Or as a MOISA Federal colleague used to say, "the juice isn't worth the squeeze.")

Increased interoperability appears to hold the most value to the operational community when it offers a means to buy down mission risk. Where lives are threatened and missions are endangered or made more complicated by lack of communication, coordination and information sharing, those are the points at which increased interoperability becomes extremely desirable to regional agencies. However, PIPS saw that regional agencies will not act on this desire if doing so seriously disrupts or takes away from what is currently working, or if it places restrictions on the complex relationships and highly nuanced information sharing that is currently relied on to build community and accomplish shared missions.

The most critical challenge facing Project Interoperability is effectively partnering with regional operational communities to build increased interoperability into their highly informal, trust-based information sharing systems. These trust-based systems are already working to build and connect operational communities as they work heroically to provide daily security and safety to the citizens and structures of their region. There is ample room for improvement, and mission-critical operational benefits can be derived from innovative design, development, introduction and evolution of new interoperability tools and concepts. However, these benefits cannot initially be achieved through mandated machine and data standards. PIPS found that technology issues were rarely the barriers to increased regional interoperability. Rather, there were numerous issues of motivation, legal concerns, community consensus, agency policies, cost, regional adoption, and mission coordination that had to be resolved before the current roster of PI tools could be applied.

In sum, this report calls for and gives an example of next generation PI tools focused on policy, community building and mission enhancement. This additional set of mission-centric PI tools and concepts will add value to and focus application of the existing machine-and-data-centric suite. This report also provides analysis, conclusions, and a plan of action to help achieve Project Interoperability's most pressing objective -- partnering with operational communities to achieve the mission benefits of increased regional interoperability.

3 Project Interoperability

The attacks of September 11, 2001 have dominated our perspective on security and safety like no other event in U.S. history. A central focus of this perspective over the past 15 years has been the critical role of information sharing and integration. As emphasized by the *9/11 Commission Report*, "The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' No one component holds all the relevant information."[8] An important component of the Federal response to this urgent call for information sharing and integration was organizational. In the largest federal reorganization since the creation of the Department of Defense, the Homeland Security Act of 2002 integrated all or part of 22 different federal departments and agencies to establish the Department of Homeland Security.

Shortly after that, another less extensive but critical organizational response to 9/11 occurred – the creation of the Office of the Program Manager for the Information Sharing Environment (PM-ISE), established under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). This was an important recognition that the ISE itself was a critical resource for the security and safety of our country, and that that this environment required promotion and guidance to grow in the desired direction of increased responsible information sharing. New and evolving partnerships are an important part of this growth.

> *PM-ISE is unique in that it possesses the mandate and the necessary tools to empower, oversee, and advance the ISE. Thanks to our many successful partnerships, the ISE continues to grow, making a significant contribution to the safety and security of the American people.*[9]

A central goal of PM-ISE partnerships has been increased interoperability within the ISE. This led to the launching of Project Interoperability (introduced in the previous section) in 2014. In its 2016 Annual Report to the Congress, PM-ISE identifies three "lines of effort," one of which is "Develop and integrate Project Interoperability (PI) and the Information Sharing and Safeguarding Core Interoperability Framework to improve information sharing and safeguarding by ISE partners across their enterprise architectures."[10] The IS&S Core Interoperability Framework (IFIC), currently described in whitepapers and a website, is an evolving framework for achieving interoperability. The IFIC uses an extremely broad and comprehensive definition of interoperability that "includes both the technical exchange of

[8] *The 9/11 Commission Report*, p. 408, July 2004.

[9] The Role of PM-ISE, https://www.ise.gov/about-ise/what-ise, accessed Sept. 8, 2016.

[10] *ISE Annual Report to the Congress* (2016), http://www.ise.gov/annual-report/, accessed Sept. 9, 2016.

information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment."[11] PIPS researchers contributed to this definition, especially its expansion to include mission accomplishment.

The IFIC views interoperability as occurring at many levels. It calls this "an 'interoperability continuum' that enables a capability-based specification of design attributes for each level of interoperability."[12] The IFIC levels of interoperability, taken from Tolk, Diallo, and Graff, are: (0) No Interoperability, (1) Technical Interoperability, (2) Syntactic Interoperability, (3) Semantic Interoperability, (4) Pragmatic Interoperability, (5) Dynamic Interoperability, and (6) Conceptual Interoperability (see Fig. 1 below).[13] Without going into the details of these levels, the point here is that interoperability covers a wide array of issues from machine to data to mission and that it exists at many levels along a capability spectrum ranging from no interoperability to interoperability that produces measurably improved mission outcomes.

The mission of PI is to promote and guide the development of ISEs to enhance national security and public safety through responsible information sharing among the numerous stakeholder partners. While this mission is broad and the IFIC conceptual framework many-leveled, PI's most concrete initial efforts have focused on specific standards that address the lower levels of its "interoperability continuum." The assumption of this approach is that PI can best guide the development of ISEs by first "advancing core frameworks and standards developed, refined, and tested through more than a decade of terrorism-related information sharing."[14]

> *The purpose of Project Interoperability (PI), a collaboration between the Standards Coordinating Council (SCC) and PM-ISE, is to promote the development of Information Sharing Environments (ISEs) between federal, state, local, tribal, and private sector mission partners at the domestic nexus of national security and public safety. Further, PI advocates for particular standards and technologies most likely to achieve the desired information sharing results and future compatibility between those ISEs.*[15]

[11] *Interoperability*, Version 1.0, Standards Coordinating Council, 12 October 2015, p. 1.

[12] Ibid.

[13] "Using the Levels of Conceptual Interoperability Model and Model-based Data Engineering to Develop a Modular Interoperability Framework." 2011, Tolk, Diallo, and Graff, *Proceedings of the 2011 Winter Simulation Conference*, p. 2576.

[14] *ISE Annual Report to the Congress* (2016), op cit.

[15] "Project Interoperability: Building a Foundation of Technological Collaboration to Support Terrorism-Related Information Sharing," https://www.ise.gov/mission-stories/standards-and-interoperability/project-interoperability-building-foundation, accessed Sept. 12, 2016.

Part of the story told by PIPS research is that, from the perspective of the operational community, the "core interoperability framework" needs to be approached differently. Rather than begin with the bottom levels of interoperability as core components to be resolved and built on – a common machine-centric approach – it is the higher levels of dynamic and conceptual alignment, captured in policy and community building and coordinated operations, that need to be resolved first and built on. With these higher level issues addressed, the lower level machine and data standards become far more valuable as the instruments for achieving the higher level conceptual agreements.

We begin this story by examining the current ten PI "tools for building information interoperability."

3.1 Analysis of Project Interoperability Tools

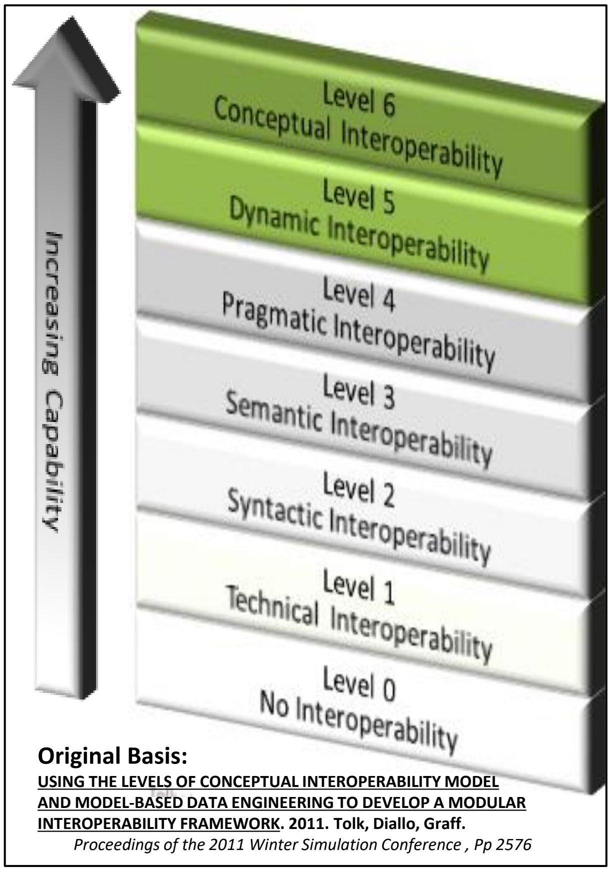
On its draft website (http://project-interoperability.github.io/) Project Interoperability presents ten "Interoperability Tools" for "building information interoperability." As part of the PIPS research, we analyzed the ten tools, selected four to explore more closely, and then addressed three questions:

(1) How useful and applicable to mission accomplishment are the interoperability tools and concepts?

(2) Why may some tools not be useful?

(3) What strategies can be used to improve tool design, usability, and outreach?

We began our analysis of the ten PI interoperability tools with the goal of focusing on those tools that were of greatest interest to the regional operational community. This turned out to be equivalent to being highest on the PI "interoperability continuum." The regional operational community that PIPS represents has far more interest in the higher, more mission-oriented interoperability layers than the lower, more machine-oriented ones. In addition, there are numerous other PI efforts, led by the SCC, that are focused at the lower levels of interoperability. From the perspective of the interoperability continuum (see Fig. 1), field operators' attention to interoperability is top-down rather than bottom-up.


Increasing Capability
Level 6
Conceptual Interoperability
Level 5
Dynamic Interoperability
Level 4
Pragmatic Interoperability
Level 3
Semantic Interoperability
Level 2
Syntactic Interoperability
Level 1
Technical Interoperability
Level 0
No Interoperability

Original Basis:
USING THE LEVELS OF CONCEPTUAL INTEROPERABILITY MODEL AND MODEL-BASED DATA ENGINEERING TO DEVELOP A MODULAR INTEROPERABILITY FRAMEWORK. 2011. Tolk, Diallo, Graff.
Proceedings of the 2011 Winter Simulation Conference , Pp 2576

Figure 1: The Interoperability Continuum

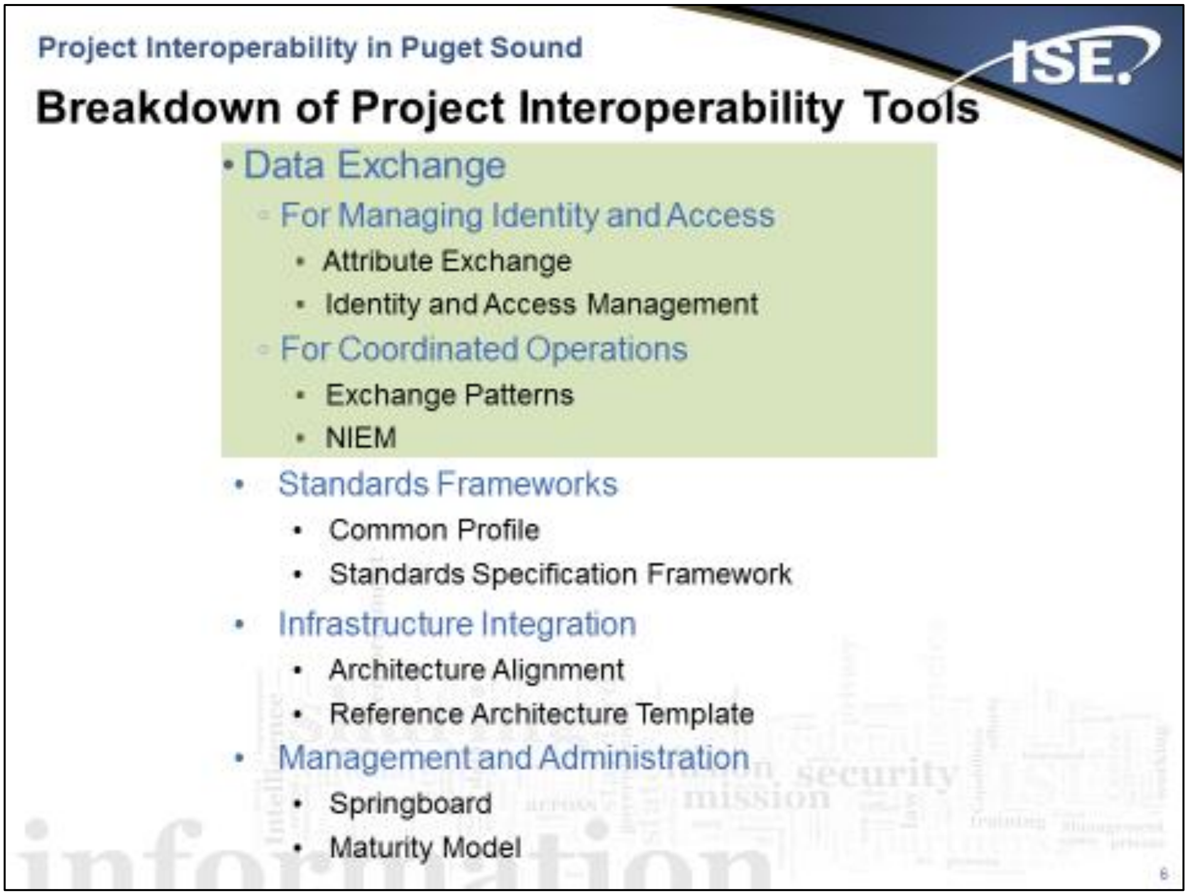
We found that the PI tools fall into four general categories: (1) tools for management and administration, (2) tools for infrastructure integration, (3) tools for standards developers, and (4) tools for data exchange. The four tools in category 4 ("data exchange") were highest on the continuum, so we focused primarily on those.

Before presenting the analysis for the four "data exchange tools" (green box in Fig. 2 below), following is a quick overview of the other six PI interoperability tools.

3.1.1 Interoperability Tools for Management and Administration

These tools are intended to help organizations manage their interoperability efforts.

Springboard. Springboard is a service operated by the non-profit Integrated Justice Information Systems (IJIS), which evaluates and certifies program compliance with information sharing standards. The implementation of Springboard in July 2012 provided the first means to verify vendor and developers' claims of compliance with information sharing standards. Springboard currently certifies compliance in justice, public safety, and homeland security communities.[16]



Project Interoperability in Puget Sound

Breakdown of Project Interoperability Tools

- Data Exchange
  - For Managing Identity and Access
    - Attribute Exchange
    - Identity and Access Management
  - For Coordinated Operations
    - Exchange Patterns
    - NIEM
- Standards Frameworks
  - Common Profile
  - Standards Specification Framework
- Infrastructure Integration
  - Architecture Alignment
  - Reference Architecture Template
- Management and Administration
  - Springboard
  - Maturity Model

6

Figure 2: Breakdown of PI tools (Ten PI Tools in Black Font)

Maturity Model. The maturity model provides a means of evaluating mission reference architecture and interoperability architecture artifacts. The ISE maturity model is broken down by the common approach (CA) domains in the Federal Enterprise Architecture (FEAF): Business, Data, Applications and Services, Technical, and Performance. Each level of interoperability is categorized in one of five levels: ad hoc, repeatable, enhanced, managed, and optimized. The goal is not necessarily to reach the 'optimized' level for each domain. Individual organizational needs will create requirements for the maturity level of each category.[17]

[16] http://www.ise.gov/blog/carrie-boyle/prove-your-interoperability-and-standards-compliance-ijis-springboard accessed 7/17/15.

[17] http://project-interoperability.github.io/maturity-model/ accessed 7/21/15.

We did not come across any awareness of the PI tools for management and administration among the Puget Sound operational community.

3.1.2 Interoperability Tools for Infrastructure Integration

These tools are intended to help organizations align their system architectures.

Architecture Alignment. Regional maritime safety and security communities are comprised of actors representing many functional and organizational organizations, using a variety of ISE architecture frameworks. Architecture Alignment is the process of creating interoperability among these architectures. Project Interoperability's efforts are not intended to drive convergence of the frameworks, but to provide a higher-level mechanism to align reference architectures.[18]

Reference Architecture Templates. A Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. Reference architecture templates assist in the development of reference architecture tools to support interoperability. The primary purpose of this tool is to guide and constrain the instantiations of solution architectures.[19]

We did not come across any awareness of these tools among the Puget Sound operational community. This was not surprising; field operators would not likely care if their plug was two or three pronged so long as they had power.

3.1.3 Interoperability Tools for the Standards Community

These tools are intended to help the standards community align their interoperability standards efforts.

Common Profile. A "Common Profile" standardizes the method of documenting an interoperability profile. This is primarily an aid to those who create, maintain and use standards to help them manage standards efforts. It provides a template for consistently documenting the contents of a profile within and across organizations. The profile being documented could run the gamut from technical specification to mission-related

[18] http://project-interoperability.github.io/architecture-alignments/ accessed 9/14/16

[19] http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf accessed 7/22/15.

process, and provides a common standards package that includes three views: reference, technical and implementation.[20]

ISE Standards Specifications Framework. The Standards Specifications Framework provides "descriptive mechanics to develop components and processes necessary to identify and normalize standards to achieve interoperability." The goal is to define a framework that helps the standards community understand an interoperability standard, the function it serves, the stakeholders involved, and the relationships across standards.[21]

Since these tools are intended for the standards community, it is not surprising that we did not come across any awareness of these tools among the Puget Sound operational community.

3.1.4 Interoperability Tools for Data Exchange

The four PI tools that are potentially most relevant to the operational regional community are tools intended to help organizations come to a common definition of data that can be shared across organizations to better accomplish mission-related activities. Data is more than just numbers or defined items in a database. Data represents the entities of interest to an organization or partnering groups of organizations. Databases that house data also represent the relationships among data types, the questions that will be answered using that data, and the methods by which the questions will be answered. In other words, tools and standards for data exchange are higher up the interoperability continuum than the previous categories of PI interoperability tools.

For this reason, we selected the four data exchange tools below for additional analysis; specifically, for each we answered the three PI tool questions introduced earlier. In addition, after further analysis, we broke these four tools down further into two sub-categories: (1) Data Exchange for Managing Identity and Access, and (2) Data Exchange for Coordinated Operations.

Data Exchange for Managing Identity and Access

The two PI interoperability tools under this category are "Identity and Access Management" and "Attribute Exchange."

Identity and Access Management (IdAM). The general concept of IdAM – confirming the identity of whom you are sharing information with and managing what they are

[20] http://ise.gov/sites/default/files/Common_Profile_Framework_v2_2015.pdf pp. 11-12 accessed 7/17/15.
[21] http://project-interoperability.github.io/standards-specifications/ accessed 7/23/15.

able to receive – is at the heart of an ISE. Some have even called IdAM the "holy grail" of information sharing, yet despite the central importance of these two processes, we cannot say that PI IdAM tools are as yet useful in Puget Sound regional mission accomplishment. The use case analyses in Section 4 provide numerous examples of regional systems with little or no formal IdAM mechanisms, or systems that employ group rather than individual logons.

There are a number of reasons why PI IdAM tools are as yet having extremely limited impact in the region. First, PI lists "Identity and Access Management" under "tools," but it is not referring to a well-defined solution that can be accessed and applied to address a given issue of identity or access. Rather, IdAM for PI is "a diverse portfolio of services and processes" that includes "all aspects of a user's digital identity lifecycle" and "allows an organization to ensure that access to its sensitive information and facilities is only granted to the appropriate individuals and audited accordingly."[22] This is a huge problem space. PI then refers to the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* which is itself a wide-ranging document that is "a call to action for ICAM policy makers and program implementers across the Federal Government to take ownership of their role in the overall success of the federal cybersecurity, physical security, and electronic government (E-Government) visions, as supported by ICAM."[23] As yet, PI is not providing concrete IdAM solutions that non-Federal agencies in the field can apply to their systems.

Second, the field's interest and ability in addressing IdAM issues is complicated by tensions between the twin ISE goals of simultaneously sharing critical information and safeguarding it.

> *Our national security depends on our ability to share the right information, with the right people, at the right time… Today's dynamic operating environment, however, challenges us to continue improving information sharing and safeguarding processes and capabilities. While innovation has enhanced our ability to share, increased sharing has created the potential for vulnerabilities requiring strengthened safeguarding practices.*[24]

[22] http://project-interoperability.github.io/idam/ accessed Sept 16, 2016.

[23] *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, v2.0, December 2011, p 2.

[24] *National Strategy for Information Sharing and Safeguarding*, December 2012.

Federally-led initiatives such as FICAM, while multi-faceted, tend to be driven from the safeguarding, cybersecurity perspective. The FICAM Implementation Guidance document begins:

> *One of the most serious security challenges that the United States faces today is the threat of attacks on its digital information and communications infrastructure. The need for effective cybersecurity is at an all-time high, while recent cybersecurity reviews, including the Cyberspace Policy Review released by the White House in May of 2009, have highlighted that the Federal Government must do more to address these threats. The Government Accountability Office (GAO) recently found that most agencies have not implemented the necessary security controls to prevent and detect unauthorized access to federal information technology (IT) networks, systems and data. Security weaknesses found included the areas of user identification and authentication, encryption of sensitive data, logging and auditing, and physical access. Identity, Credential, and Access Management (ICAM) efforts within the Federal Government are a key enabler for addressing the nation's cybersecurity need.*[25]

While Federal agencies that operate in the region tend to be sensitive to these safeguarding issues, many local agencies are much less so. These local agencies build community and information sharing environments outside the formal systems that are the prime candidates for application of FICAM initiatives. Regional operational entities are continually developing and exercising relationship and trust based networks for sharing information that are not only more nuanced than formal systems (e.g., "you didn't hear this from me but…") but are also secure, because they are built on personal and agency capital developed over years of working together. Such an effective, informal ISE cannot easily accommodate more security-focused approaches relying on credentialing of people and classification of information.

Regional professionals view Federal initiatives as overly focused on safeguarding to the detriment of mission-based sharing. Towards the end of the PIPS project, we presented an overview of these results at the annual Maritime Security West conference. Having presented the idea of a "top-down" approach to regional interoperability based on a mission-centric perspective, we engaged regional security professionals in discussion. The general sentiment was that they would be happy to participate in the design and use of a regional system that enabled them to better send and receive useful information,

[25] *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, v2.0, December 2011, p 1.

but they feared that the system would be owned by "the Feds" who would "just lock it down and drive us crazy with passwords and other restrictions."

Another example of this challenge to Federal IdAM solutions at the regional level occurred during the DHS Integrated Maritime Domain Awareness/Coastal Surveillance System (IMDE/CSS) project that was taking place in the Puget Sound during PIPS. IMDE/CSS is not specifically an IdAM initiative; it is an effort to develop and exercise a pilot enterprise architecture that will enhance the ISE by putting data and applications on a shared regional backbone. The IMDE architecture is compelling from a regional standpoint because it has the potential to eliminate technical barriers to information sharing without requiring local agencies to give up their individual systems.

But while IMDE/CSS is not an IdAM initiative, it has presented the challenge of addressing IdAM issues as well, since any effort to foster a community of users capable of accessing and sharing data and operational information over a shared enterprise backbone must consider the processes for gaining entrance to that community and for managing access to data and applications. For its initial demonstration, the IMDE team followed DHS requirements that users who wanted access to the system but did not meet certain criteria would have to go through a self-funded security background check. This was an instant non-starter for the local community, who once again saw federal safeguarding requirements raising roadblocks and outweighing the need to foster participation and facilitate information sharing.

In summary, the current PI IdAM toolset is not yet providing concrete solutions that will work in the regional environment. This can be remedied by redirecting future PI IDAM initiatives towards more "top-down" mission-centric efforts. These efforts must partner with the regional community to develop less formal IdAM tools that leverage existing information sharing relationships. An example of such a tool is in Section 3.2.1.

Attribute Exchange. Attribute exchange is an approach to identity and access management based on the exchange of user attributes between an "identity provider" (IdP) and a "service provider" (SP). Attribute based access control (ABAC) is a method of providing access to a service based on an evaluation of a user's attributes. The basic architecture (there are many variations) is that the user identity attributes live within the IdP and, after a user attempts to access a service, the SP sends an authorization request to the IdP. The IdP exchanges the user identity information with the SP through the use of secure tokens, the SP evaluates those attributes, and the access is, or isn't, granted.

One issue here is achieving inter-organizational agreement on the attributes that describe identity, as well as the precise description of those attributes. Considerable work has been done in this area, but as NIST says,

> *Over the past decade, vendors have begun implementing Attribute Based Access Control (ABAC)-like features in their security management and network operating system products, without general agreement as to what constitutes an appropriate set of ABAC features. Due to a lack of consensus on ABAC features, users cannot accurately assess the benefits and challenges associated with ABAC.*[26]

The most common version of the specification by which user identity attributes are exchanged is the Security Assertion Markup Language (SAML—pronounced "Sam L"). SAML is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It is a product of the OASIS Security Services Technical Committee, a member of the Standards Coordinating Council.

SAML has evolved into a powerful standard for addressing the issue of agreement on identity attributes, but it is also important to realize what it does not address. Attribute exchange languages like SAML describe and carry the identity attributes, but not the policies and practices that determine what will be done in terms of service access and information sharing given those attributes. This issue may seem relatively minor if the only question is access, that is, if you are Google and your only question is whether or not to give someone access to your services. It is far more complicated and central, however, for the security and safety community, whose information sharing issues are far more pragmatic, requiring more differentiation and situational awareness.

> *Like every hammer brought to bear on a screw, [SAML] falls short a bit. If all you need to do is pass attributes into the application, then SAML will help for sure. But if you're looking for a way [to] express and store policy about the content of those attributes and what the resultant set of decisions should be based on the expression of those policies, then you're out of luck.*[27]

[26] "Attribute Based Access Control (ABAC) – Overview," NIST, (May 2015), http://csrc.nist.gov/projects/abac/, accessed October 3, 2016.

[27] Sander, Jonathan, "SAML vs XACML for ABAC & AuthZ," March 9, 2010, https://identitysander.wordpress.com/2010/03/09/saml-vs-xacml-for-abac-authz/, accessed Oct. 4, 2016.

These "policy expressions" that drive decisions about identity and access management live not on the IdP, but on the service provider side of the architecture, and much work needs to be done to create a functional language of policy expressions.

Another issue for attribute exchange that goes beyond what SAML addresses is the possibility that agencies will employ group rather than individual logins, especially during disaster response. This practice occurred during the recent Cascadia Rising Exercise (see Section 4.2) when the need to use new systems and share information across new partners led regional agencies to assign group rather than individual logins. There are advantages to group logins (quicker access for more people; easier to track what your team is doing) but group logons cannot fully employ current approaches to attribute exchange.

Overall, attribute exchange as a PI tool mirrors what was found in the analysis of the current PI tools in general. While SAML has gone a long way towards addressing the basic exchange of identity attributes, there is a need to put this tool in the context of mission-based expressions of organizational IdAM policy that have not been as thoroughly addressed. Just as the overall PI tool set needs greater emphasis on top-down, mission-centric approaches, so too do efforts to advance attribute exchange need to put greater emphasis on the policy side of IdAM and the situational considerations of mission-centric information sharing.

Data Exchange for Coordinated Operations

The two PI interoperability tools under this category are "Exchange Patterns" and "the National Information Exchange Model" (NIEM).

Exchange Patterns. Even though exchange patterns are listed on the draft PI website as a tool, they are as yet loosely defined components of a generic concept of an "information exchange specification." These exchange pattern components are not yet ready for prime time as tools that an operational regional community could use to enhance their security and public safety mission.

The idea behind exchange patterns is to identify a set of core functions and repeatable tasks within an information sharing transaction, and "describe and catalog [those functions] along with interoperability technical standards and services requirements as part of an information exchange specification."[28] The present scope of this initiative is too broad to resolve quickly into useful tools. Core functions cover everything from "an evolved governance model" to agreement on interoperability requirements to "a

[28] *ISE Information Interoperability Framework (I^{2}F)*, Version 0.5, March 2014, p. 13.

standardized way of developing patterns that project teams may implement as they develop their mission-specific applications."[29] The exchange pattern components described in the I^{2}F (v. 0.5, March 2014) constitute a dizzying array of overlapping functions and issues that include: Standardized Interfaces and Interoperability, Query/Response Patterns, Broadcast Patterns, Workflow Patterns, Coordination Patterns, Context and Use of Process Rules, Context and Use of Data, Context and Use of Services, Context and Use of Policy, Exchange Specifications, Federated Identities Patterns, Identity Exchange Patterns, Federated Identities, and Federated Queries Patterns.

On a more positive note, with such a broad scope and wide array of issues, the exchange patterns initiative could easily focus more on the mission-centric issues at the top of interoperability continuum, and move PI in a desirable direction from the standpoint of the regional operations community. One possibility is to focus on the workflow patterns of critical regional missions, and use that workflow to identify common pain points that could be addressed through the evolving PI tool suite. An example of this can be seen in the workflow modeling of port security screening of cargo containers described in the year one MOISA report.[30]

National Information Exchange Model (NIEM). While NIEM is listed by Project Interoperability as one of the ten PI Tools, it is an initiative that existed long before PI and that extends far beyond PI. Federal efforts to standardize data exchange in support of inter-agency information sharing are about fifteen years old, starting in both DHS and the Department of Justice (DOJ). NIEM was formally initiated in 2005 by the CIOs of DHS and DOJ, and in 2010 the Department of Health and Human Services joined as a third sponsoring agency.

NIEM is a very visible program at the Federal level. It is recognized in the *National Strategy for Information Sharing and Safeguarding* as "a successful example of a common way to structure data exchanges to better enable information sharing"[31] and is selected as a central strategic component of the Maritime Information Sharing Environment (MISE).

> *Through the definition of data standards within the National Information Exchange Model-Maritime (NIEM-M), the MISE provides a common vocabulary in four initial focus areas: Vessel Positions, Advance Notice of Arrival, Indicators*

[29] Ibid.

[30] *Maritime Operational Information Sharing Analysis*, September 2014, pp. 82 – 95. http://www.hcde.washington.edu/files/news/MOISA1-Final-Report.pdf?pdf=MOISA-Year-1

[31] *National Strategy for Information Sharing and Safeguarding*, December 2012, p. 4.

> *and Notifications, and Maritime Operational Threat Response. While only four focus areas are defined in the initial effort, the standards and processes defined by the MISE are designed to be reusable and extensible to support future information sharing products and partners.*[32]

In addition to the maritime domain, NIEM initiatives exist, in varying degrees of maturity, within fourteen other "sectors:" (1) Emerging Communities; (2) Biometrics; (3) Chemical, Biological, Radiological and Nuclear (CBRN); (4) Children, Youth and Family Services (CYFS); (5) Emergency Management; (6) Human Services; (7) Immigration; (8) Infrastructure Protection; (9) Intelligence; (10) International Trade; (11) Justice; (12) Military Operations; (13) Screening; and (14) Surface Transportation.

Despite this long history, breadth of scope, and recognition at the Federal level, we did not find NIEM to currently be a significant factor within the Puget Sound regional operational ISE. We found one NIEM pilot project, conducted in 2008 and funded by the National Governors Association ($50,000), that established a NIEM-conformant Information Exchange Package Documentation (IEPD) for the exchange of Washington State driver's license photos. Other than this "case study," as NIEM calls it on its website (www.niem.gov), NIEM was never identified as an ISE factor in any of the hundreds of interviews conducted and meetings attended by MOISA and PIPS researchers over the past three years.[33] In fact, during our Use Case study of post-disaster resource requesting and tracking (see Section 4.2 below), we specifically asked developers of the Washington Information Sharing Environment (WISE) system, working at the Washington Army National Guard (WANG), if they considered NIEM in the creation of their database. Not only had they not considered it, they hadn't even heard of it.

NIEM is the most extensive effort of the "PI tools," but even it has not yet had a significant impact on the regional security and safety information sharing environment. NIEM too would benefit from a more top-down approach that emphasizes the upper levels of the interoperability continuum, for example generating its data definitions not from a panel of sector experts, but from working with regional partners to map the work

[32] *The National Maritime Domain Awareness Architecture Plan*, Version 3, Release 2, 2015, p. iv.

[33] In year one, for example, MOISA conducted 77 formal interviews with individuals representing 52 organizations active in the Puget Sound ISE.

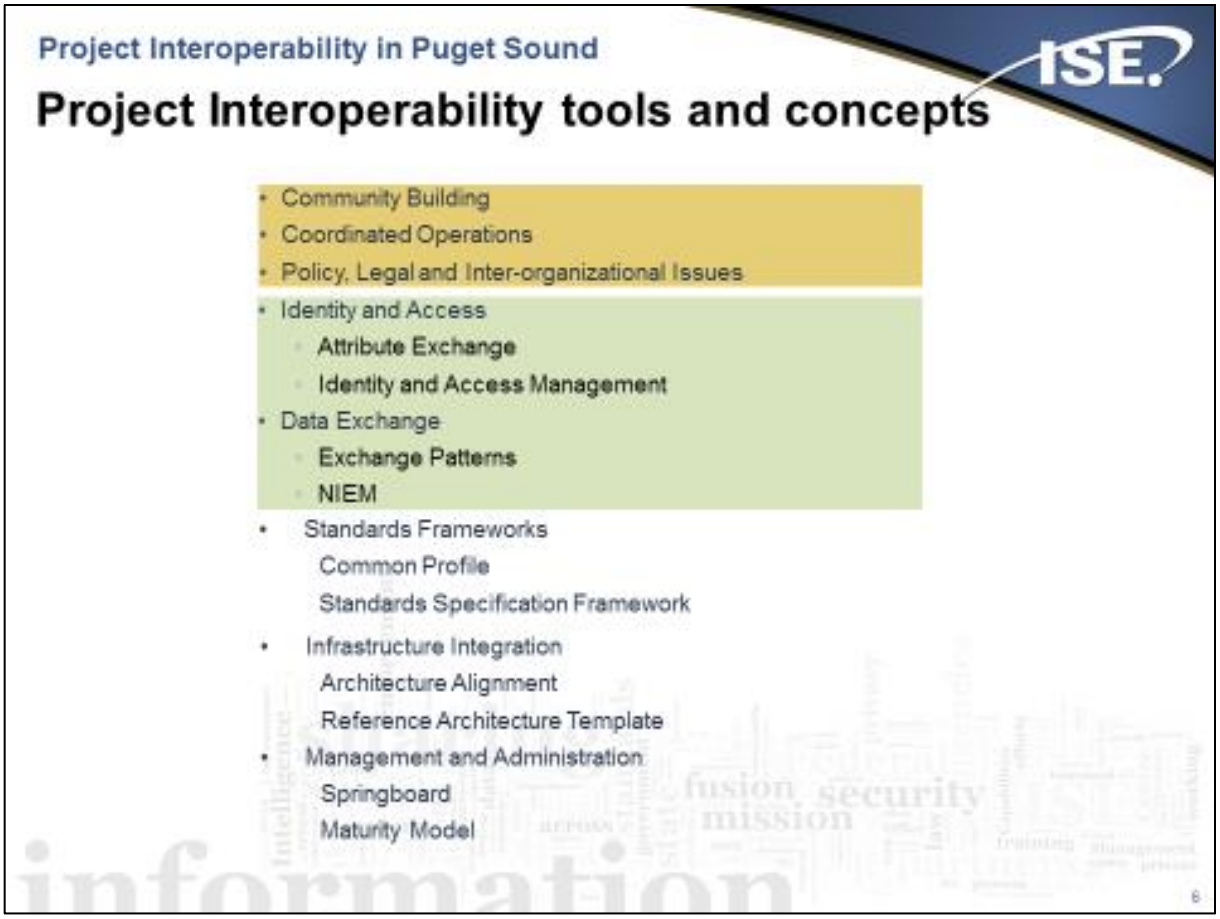
itself (see, for example, the generation of a data dictionary from workflow mapping of port security processes described in the Year One MOISA report[34]).

Project Interoperability initiatives require an expansion of scope that includes partnering with operational agencies to identify and add tools that are community-based and mission-focused, going beyond machine and data to include policy, legal, organizational and other non-technical issues. The following section provides an example of such a mission-focused "gold tool."

3.2 Towards Community-based, Mission-centric Project Interoperability Tools

As discussed in Section 3.1.1, the regional operational community has far more interest in the higher, more mission-oriented interoperability layers than the lower, more machine-oriented ones. Lacking in the current set of ten PI tools are community-based, mission-centric interoperability tools to facilitate community building, enhance coordinated operations, and incorporate the policy and legal requirements necessary for information sharing and safeguarding. Therefore, we propose a shift in effort to the development of a next generation of community-based, mission-centric interoperability tools that we refer to here as the "gold tools" (see Figure 3). This set of tools would be highest on the PI "interoperability continuum" (see Figure 1) and would motivate regional interoperability partnerships by addressing the interoperability needs of field operations.

[34] *Maritime Operational Information Sharing Analysis*, Op Cit.



Project Interoperability in Puget Sound

Project Interoperability tools and concepts

- Community Building
- Coordinated Operations
- Policy, Legal and Inter-organizational Issues
- Identity and Access
  - Attribute Exchange
  - Identity and Access Management
- Data Exchange
  - Exchange Patterns
  - NIEM
- Standards Frameworks
  - Common Profile
  - Standards Specification Framework
- Infrastructure Integration
  - Architecture Alignment
  - Reference Architecture Template
- Management and Administration
  - Springboard
  - Maturity Model

6

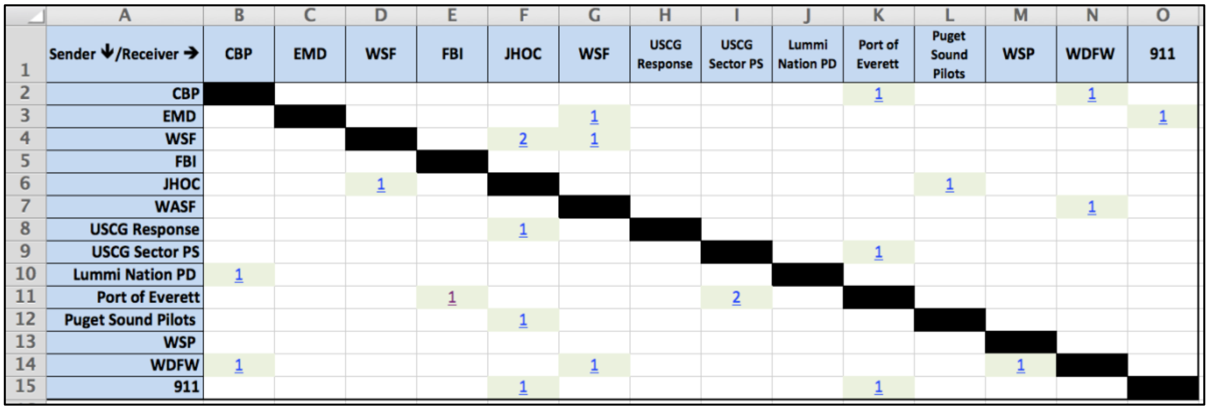
Figure 3: Project Interoperability Tools and Concepts

We present in the next section an example of a gold tool that would build on the existing trust and relationship-based regional ISE to support development and a new kind of ISE IdAM layer.

3.2.1 The Information Sharing Matrix

The Information Sharing Matrix is a proof of concept depicting the information sharing relationships among agencies within the Puget Sound region. Understanding who should have access to which data at what times and for what reason is critical to developing a next generation, mission-centric interoperability tool. The information-sharing matrix is a framework for capturing the existing trust relationships necessary to the design and development of an identity and entitlement management layer.

The data for this prototype came from CoSSaR's MOISA Year 1 project. Interviews were conducted with approximately 70 Puget Sound maritime agencies and these interviews were then analyzed for sharing relationships. Relationships from 14 example agencies are represented in the *Information Sharing Matrix* Excel worksheet in Fig. 4, below.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Sender ↓/Receiver →	CBP	EMD	WSF	FBI	JHOC	WSF	USCG Response	USCG Sector PS	Lummi Nation PD	Port of Everett	Puget Sound Pilots	WSP	WDFW	911
2	CBP	■									1			1	
3	EMD		■				1								1
4	WSF			■		2	1								
5	FBI				■										
6	JHOC			1		■						1			
7	WASF						■							1	
8	USCG Response					1		■							
9	USCG Sector PS								■		1				
10	Lummi Nation PD	1								■					
11	Port of Everett				1				2		■				
12	Puget Sound Pilots					1						■			
13	WSP												■		
14	WDFW	1					1						1	■	
15	911					1					1				■

Figure 4: Example of Matrix Showing Information Sharing Relationships

Each row in Fig. 4 represents the agency sending the information and each column represents the agency receiving the information. If sub-units of a complex agency (e.g. USCG Response) exhibit their own patterns of information sharing, they are treated in the matrix as a separate agency. If Agency A shares information with Agency B, the cell with row A and column B is highlighted with a hyperlink to the information sharing incident. For example in Fig. 4, cell B10 shows that the Lummi Nation Police Department sends information to Customs and Border Patrol (CBP).

Each agency has its own Excel worksheet (as a sender) that includes the instances of the agency sharing information with other agencies. The number displayed in the cell represents the number of information sharing incidents that occurred between Agency A and Agency B. The number in the cell links to the appropriate sender worksheet where the details concerning the information-sharing incident are stored. For example, in cell B10 there is a "1," which opens the *Lummi Nation PD* sender worksheet (Fig. 5) displaying the example of information sharing that occurred between the Lummi Nation PD and CBP. In this example, the number 1 indicates we have only provided one example, but there could be numerous examples for each sharing relationship.

The sender worksheet (Fig. 5) contains the details of the information-sharing incident as it was recorded during the MOISA 1 interview. The Source Document column contains the filename for the information-sharing incident, should there be a need to return to this information to gather additional information/insight, while the Excerpt Copy column provides the details of the information sharing incident. Additional columns of this worksheet are Receiving Agency (e.g., CBP), Medium (e.g., phone), Interoperability (data-centric, mission-centric), and Pain Points (any noted difficulties in achieving information sharing and interoperability). These categories could be expanded or modified as the matrix concept matures.

Source Document	Excerpt Copy	Receiving Agency	Medium	Interoperability	Pain Point
12.19.2013_CBP_Michael Hoffman_INT_V1_MD_MOISA	Tribal - Ron Tso: in charge of Police Dept. - Deal with tribes a lot with crabbing vessels - Call CBP. Tribes doing this to warn them, tribes keep the CBP informed - Tribes have law enforcement boats - Tribal police are trusted - Problems: Tribal vessel registration has to go through the tribes (complication wall) Biggest pain point. Paper registration. - Tribal IDs. Have to get this information from the tribes	CBP	Phone Face-to-face	Mission-centric	Paper-based system for vessel registration

Figure 5: Lummi Nation PD Sender Worksheet

This particular example shows the information sharing of vessel registration IDs that occurs between the Lummi Nation Police Department (PD) and Customs and Border Patrol (CBP) via a paper-based system. While technology could be developed to replace this paper-based system and data-centric interoperability tools could be deployed to facilitate the exchange of vessels registration IDs between the two parties; this does not guarantee interoperability. Mission-centric interoperability must be addressed first to coordinate missions, align policies and build community. Only when this higher conceptual level has been addressed, can the data-centric and machine-centric tools be deployed.

The sections below further support this approach, first through examination of interoperability in the context of the two use cases: 1) planning and scheduling of daily operations and 2) resource requests and tracking during emergent events in the Puget Sound region.

4 Use Cases

PIPS employed the concept of "use cases" as it is used in agile, human centered design methodology.[35] In this sense, a use case is a broad mission that can be used to examine workflow, organization, policy and other issues that affect how people accomplish their mission. In many ways, PIPS was a continuation of a project that immediately preceded it—the Maritime Operational Information Sharing Analysis (MOISA).[36] During MOISA, we began an analysis of a use case on interagency planning and scheduling. This use case was part of our design contribution to a DHS S&T Borders and Maritime initiative to pilot an enterprise architecture and associated capabilities in the Puget Sound—the Integrated Maritime Domain Enterprise/Coastal Surveillance System (IMDE/CSS).

Under MOISA, researchers and designers at CoSSaR began working with software developers at SRI International to engage the Puget Sound operational community in human-centered, agile design and development of the planning and scheduling capabilities of IMDE/CSS. PIPS leveraged this work using it as the basis for the first of two PIPS use cases, the other use case being post disaster resource requesting and tracking. We selected these two use cases, in part, so that our in-depth analyses would cover both daily operations and post-disaster emergency response.

4.1 Use Case One: Planning and Scheduling Capabilities

The Planning and Scheduling use case examines information sharing and interoperability for actors in the Puget Sound who coordinate resource use in support of maritime activities. Our analysis was two-pronged, focusing on (a) the as-is processes for planning and scheduling and (b) mission-based opportunities for information sharing enhancements, including the possible use of interoperability tools to support these processes. We drew on data from the MOISA project's study of the regional ISE, as well as field interviews and focus groups conducted as part of iterative prototyping activities in support of development of a Planning and Scheduling module for IMDE/CSS.

[35] See for example, ISO 13407.

[36] Maritime Operational Information Sharing Analysis (2014) http://www.hcde.washington.edu/files/news/MOISA1-Final-Report.pdf?pdf=MOISA-Year-1; MOISA 2: Fostering Regional Partnerships and Innovation for Maritime Security, Safety, and Resilience (2015), http://www.hcde.washington.edu/files/news/MOISA2-Final-Report.pdf .

4.1.1 As-is Process Analysis

The focus of our as-is analysis was on both single-agency and multi-agency planning processes. We tracked and analyzed the information on which participating Puget Sound regional maritime actors currently rely to create and update their own agency plans and schedules, as well as how these actors share information to facilitate interagency planning and scheduling. Our investigations elicited information exchange patterns for each type of planning, as well as how interoperability tools enable or have the potential to enhance this information exchange.

Single Agency Planning: Interoperability in Marine Patrol Scheduling

For the single agency based investigation, we explored marine patrol scheduling by six federal and local security and safety agencies: (a) Skagit County Sheriff's office, (b) King County Sheriff's Office, (c) United States Coast Guard, (d) DEA, (e) East Jefferson County Fire & Rescue and (f) Port of Everett Security. This analysis revealed a wide diversity in ISE systems and processes among these agencies. Table 1 below summarizes the varying and independent use of systems and other information sources as identified through interviews within the six agencies. (We did not revisit this list of resources generated through initial interviews to ask if agencies used resources they hadn't mentioned. This would undoubtedly have added additional "Xs" to the table.)

Table 1: Resources Used by Selected Regional Agencies

	East Jefferson County Fire & Rescue	DEA	Skagit County Sheriff's Department	USCG	King County Sheriff's Department	Port of Everett Security
ALMIS				X		
AOPS				X		
Blue Force Tracking	X			X		
Cargo manifest						X
CGMS				X		
Email	X	X	X	X	X	X
Excel schedule	X		X			
Eyes on scene	X					
Fusion Center bulletins						X

Hand written notes transcribing info from classified system				X		
High Intensity Drug Trafficking Area (HIDTA) – by phone		X				
HSIN notes via email						X
Interagency Action Plan (IAP)	X			X	X	
In-person joint planning meetings						X
InTime ISE Scheduling software			X			
MHS-OPS				X		
New World Systems CAD	X					
Operations schedule						X
Outlook Calendar				X		
Radio	X		X		X	
Ship's schedule						X
Spillman Mobile AVL Mapping			X			
Staff schedule on whiteboard				X	X	
Telephone / Cell / Text	X	X	X	X	X	X
Western State Information Network (WSIN) – by phone		X				

Our initial interviews identified twenty-five information resources for planning and scheduling among six agencies, underscoring the diversity of the regional IES. In order to highlight this diversity, we include some details on three of the six participating agencies. By examining just a handful of organizations, it I clear that regional agencies use unique systems and processes that often don't overlap and that this presents challenges to interoperability.

Skagit County Sheriff's Office (SCSO)

An evaluation of the SCSO provided a rich example of the role of interoperability in marine patrol scheduling. SCSO consists of several units including traffic, K-9, undercover/drug task force, boat, and search and rescue. To coordinate the different unit schedules, SCSO uses the *InTime Scheduling Engine (ISE*) Enterprise.*[37] ISE* offers scheduling, overtime management, time and attendance, employee self-serve, notifications and leave management. ISE* is accessible over the Internet, and deputies can access it in their cars.

[37] http://www.officer.com/product/10049653/intime-solutions-inc-intime-scheduling-engine-ise

ISE* is built on the Java 2 Platform, Enterprise Edition (J2EE) which adheres to the Java slogan of "write once, run anywhere." J2EE is a software framework and provides developers with a set of application programming interfaces (APIs). J2EE is platform independent and will run on local area networks, wide area networks, and the Internet. Through the Java Database Connectivity (JDBC) API, it can connect to enterprise-level SQL databases including Oracle, SQL Server, and DB2. ISE* supports web services which "provide a standard means (XML, SOAP, WSDL, and UDDL open standards) of operating between software applications running on a variety of platforms and frameworks."

SCSO's use of ISE* does not take full advantage of all these interoperability options. (This gap between technical capabilities and actual use is the norm rather than the exception.) For SCSO's marine specific annual schedule, only a Microsoft Excel spreadsheet is used. Events/patrols must be manually entered. Information comes from emails, phone calls, information sharing events, the Maritime Intelligence Group (MIG), and the Tactical Action Group (TAG). The marine schedule includes day, time, vessel name, whether another agency will ride along, contact information for crew, and the assigned body of water. All marine officers can read and write to the Excel marine schedule file. East Jefferson Fire Rescue also uses Excel, with an in-house subprogram, to track hours.

If desired, excel files can be locked and/or password protected. The file can also be placed on a password protected shared drive. An Excel spreadsheet can be saved in a number of formats including XML data, web page, text, comma separated values (CSV), data interchange format (DIF), PDF, and OpenDocument Spreadsheet. Excel is also interoperable with the other MS Office products, such as Access.

King County Sheriff's Office (KCSO)

In contrast, KCSO deputies use a physical whiteboard to keep track of scheduling. Access is controlled through physical access controls to the Sherriff's Office, and officers take pictures of the whiteboard for referencing and sharing. KCSO also maintains a schedule in Atlas[38], a web-based scheduler that is platform-independent and works in any browser. Atlas serves as the human resources time keeping system where employees log their hours and vacations. KCSO also incorporates special events into

[38] http://atlasworkforce.com/sched.aspx

their scheduling, and special events permits are requested through the KCSO webpage, email, and phone.

The King County marine patrol unit, a unit within the Sheriff's Office, stated that they did not use Atlas and that they do not enter the information on the whiteboard into Atlas. This shows diversity even within given local agencies.

United States Coast Guard (USCG)

Finally, although the USCG can be viewed as a single agency, it has a complex organizational structure relative to other regional actors, and the coordination of plans and schedules among the USCG Command Center, Sector Puget Sound, and local Stations is somewhat intricate. The Sector Law Enforcement Division (ED) manages planning on a weekly basis. This results in a Weekly Plan to Execute Orders (weekly plan) that includes planned escorts and vessel boardings. The USCG escorts Navy vessels and commercial vessels, such as ferries, cruise ships, and cargo vessels. Requests for USCG high value unit (HVU) transit escort support are completed through the web-based Maritime Homeland Security Operational Planning System (MHS-OPS). MHS-OPS can only be accessed on SIPRNeT in the Joint Harbor Operations Center (JHOC). Relevant information to ED must be handwritten and reentered into the weekly plan.

CG stations put their weekly schedules in the Asset Logistics Management Information System (ALMIS). The CG Air Stations also make requests for marine assets through ALMIS. ED reported that different stations keep separate schedules in Outlook and cannot see each other's schedules. The ED draws information from phone calls, emails, MHS-OPS, and ALMIS and manually integrates these into weekly Execute Orders. This weekly plan is shared via email and distributed via the Coast Guard Messaging System (CGMS) as a courtesy. As the week unfolds, changes are made to the weekly plan, but it is generally too much trouble to reissue.

ALMIS is a USCG system that is currently undergoing modernization and will be renamed Coast Guard Logistics Information Management System (CG-LIMS). CG-LIMS will support all USCG aircraft and nine types of boats by 2018. Currently, ALMIS is not interoperable with Outlook, which USCG personnel reported using for division schedules and the Sector schedule. Data cannot be transferred between ALMIS and Outlook without manual reentry.

Multiagency Planning: The Incident Action Plan (IAP) and Data Standardization

The as-is state for interagency collaborative planning processes includes a variety of the above mechanisms. Agencies access information stored in their own agency schedules in combination with additional information resources that support collaboration with neighboring agencies in order to plan and schedule interagency operations. An important regional mechanism for coordination and information sharing related to interagency planning is the Incident Action Plan (IAP).

Our interviewees reported using the FEMA IAP forms and planning guide[39] to plan interagency operations. These forms are often filled out on paper and then scanned and transmitted via email, which recipients often need to print and share in hardcopy again. This manual work is in addition to the manual integration actions that 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 often is to combine IAP pieces into a single cohesive plan and then distribute this to other agencies participating in the operation.

The head of the Enforcement Division presented a compelling case for enhancing mission and greatly reducing overhead tasks through increased interoperability and information sharing. In the as-is case, if the weekly plan changes after distribution via email and other individualized methods, it is not even redistributed because the process is so cumbersome. Maps are particularly time consuming to produce and there is no easy sharing and integration of the geo-location information. There are numerous other non-value adding tasks stemming from the lack of shared systems and information.

[39] https://www.uscg.mil/hq/cg5/cg534/nsarc/FEMA%20Incident%20Action%20Planning%20Guide%20(IAP).pdf

	Access Control	Identification	Cybersecurity	Risk Management	Policy
911 Call Center / Dispatch	None	Caller ID	None	Do not speak about sensitive information unless it is an emergency	County coordinating bodies
Coast Guard Suite of tools: ALMIS, CGMS, Classified Network MHS OPS	Internal Coast Guard procedures	Internal Coast Guard procedures	Internal Coast Guard procedures	Internal Coast Guard procedures	Internal Coast Guard procedures
E-mail	Access limited through email addresses/lists	User may be identified through email address	Potential e-mail encryption	Do not transmit sensitive information unless it is an emergency	Each organization
IAP	Access limited through email addresses/lists	IAPs are emailed, user can be identified through email address	Potential e-mail encryption	None	Informal agreements
Meetings	Physical Security	Identification Cards Recognition of counterparts	None	None	Various
Radio	None	Self-identification of users over radio communications	Potential use of anti-jamming technology	Do not transmit sensitive information unless it is an emergency	Organization from county to federal
Telephone and Cell Phone	Unlisted numbers may limit access	Recognize voice Use phone number authenticated to the intended recipient (from business card, website)	None	Do not speak about sensitive information unless it is an emergency	Informal

Table 2: Functional Areas of Interoperability in Scheduling and Planning

4.1.2 Mission-based Opportunities for Interoperability

Unfortunately, the wide diversity of ISEs and work processes among the regional agencies who are involved in an IAP would make it difficult to address opportunities such as a digital IAP, especially given the current PI interoperability toolsuite. Before these tools can be useful, a significant number of higher-level policy and coordinated process issues need to be resolved by the operational community. Table 2 above gives an overview of how a number of systems in use by regional agencies vary across five functional areas: access control, identification, cybersecurity, risk management, and policies. These are highly dynamic and complex areas and the table presents just a general snapshot in time, not definitive attributes. The goal in presenting this table is to give a sense of the many adjustments at many levels that agencies would have to make in order to align these systems in a given coordinated mission. Even if agencies had access to a common tool (i.e., a digital IAP), each agency would approach such a tool differently. This makes sense, as agencies will conduct internal operations per their mission and organizational structure, and the possibility of standardization of the data that is used for these tools is generally an add-on secondary consideration.

There are, however, some strong mission-based incentives for standardization of some data for the purpose of facilitating cross-agency information sharing. For instance, implementing a platform for automating paper forms (such as IAPs) would reduce the amount of time required for updating, making it more likely that updates will be shared. Another strength of a common digital IAP is that over time it would become a template, with agencies likely evolving their data into a similar format to other agencies. In the event of an emergency, information could then be more easily shared if desired.

In general, a major challenge to regional interoperability initiatives is that they require amending existing internal systems that currently work well for daily operations. Agencies are less likely to adopt uniform reporting systems if doing so seems like it will disrupt the current systems that work well. It's important to point out that the goal of IMDE/CSS is to not change existing internal systems but to standardize the enterprise architecture so that data can be shared with other agencies from diverse applications. Still, even if this is accomplished, there would still be necessary adjustments to existing work processes.

In the end, improved interoperability can't occur until non-technical changes are made that support the leap to standardized data reporting within systems. Our research concluded that it's difficult to coordinate data across agencies without coordinating organizational missions first. What is needed is a large, collaborative effort at the mission, policy and organizational level, which will facilitate digital reporting systems and data standardization down the road. Given the current diversity of technology and existing internal systems, a non-technical approach is needed to gain regional agreement on mission collaboration within the security community.

4.1.3 Conclusion

The analysis of this use case provided insights into factors that impact the design of planning and scheduling business processes and system enhancements. Opportunities for mission benefits were identified, but so were considerable non-technical obstacles to achieving those benefits. Findings related to interoperability were 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; that data standardization is a gold standard that can't be accomplished until organizational missions are consolidated; and that common core information attributes transcend the boundary between pre-planned and emergent events.

A qualitative analysis described in section 5.1.1 uses the data collected during this Use Case to provide additional insights into the interoperability issues involved in planning and scheduling.

4.2 Use Case Two: Resource Requesting and Tracking Post-Disaster

This use case examines interoperability in the context of resource requests and tracking during emergent events in the Puget Sound region. The use case integrates information from a three-phase investigation:

Phase 1: Review of after action reports related to four emergent events prior to 2016.
Phase 2: A series of targeted interviews with key informants related to those previous events and also connected to the Cascadia Rising (CR) exercise.
Phase 3: Detailed observations in the Washington State Emergency Operations Center and in the Washington National Guard Joint Operations Center during the CR exercise.

The four emergent events considered in this study include two planned exercises (the 2012 Evergreen Quake exercise and the 2016 Cascadia Rising exercise) and two unplanned events (the 2014 Oso landslide, and the 2015 wildfires in Washington State).

The study centered on two key systems in the State of Washington related to achieving interoperability for resource requests and tracking in emergent events: the Washington State WebEOC and the Washington Information Sharing Environment (WISE). An additional system, ROSS, is included in the analysis because of its applicability to one of the emergent events (2015 wildfires).

The focus of this examination of the two systems in the context of emergent events is on interoperability to support information sharing among organizations. Tools and concepts related to interoperability, including an analysis of their usefulness and opportunities for development, are reported in this section of the report. Tools and concepts of central concern to PIPS' overarching goals are weighted heavily in the following analysis.

4.2.1 Emergent Events Overview

The four emergent events considered in this study include two planned exercises and two unplanned events.

2012 Evergreen Quake Exercise

The 2012 exercise scenario included five earthquakes in the Puget Sound region in Washington State occurring simultaneously across six counties. The earthquake magnitudes ranged from 5.7 to, 7.4 and occurred at 0800 on June 4, 2012. The Federal

Emergency Management Agency (FEMA) Regional Response Coordination Center (RRCC) was activated on June 5, 2012 (to simulate a 24-hour post-event start) to level one and Emergency Support Function (ESF) 11 responded to manage the ESF 11 Desk. On June 5, estimates were 2,000 deaths, 18,000 injured, 33,000 buildings damaged, 96 state highway routes damaged, several major bridges in Seattle were closed, and the Emergency Alert System was out. All Ports between Bellingham & Olympia were closed, 911 Network Power was out, and a reported 1,764,503 people were affected. Seattle-Tacoma International Airport established temporary air traffic control, had one functional runway, and diverted flights to Portland, OR. Personnel from multiple cities and six counties, state agencies, federal agencies, Tribal nations, private industry and non-governmental organizations all participated in this exercise by creating exercise injects, activating their Emergency Operations Centers (EOC) and sending representatives to participate at State or Federal Response Coordination Centers. The exercise was designed to examine EOC response actions due to a wide-area catastrophic earthquake. A related Logistic Exercise was conducted June 12-14, 2012 and a Recovery Exercise was conducted August 15 and 22, 2012. The Washington National Guard (WANG) conducted an internal, follow-on exercise for earthquake response, Evergreen Tremor, in June 2015.

WebEOC (at the state level) was used during the exercise and users recommended changes to the system, which have since been implemented.

2014 Oso Mudslide (SR530 Landslide)

On March 22, 2014, a major landslide occurred near the town of Oso, WA resulting in 43 deaths and 49 homes and structures being destroyed. The landslide also dammed the Stillaguamish River, which resulted in flooding and the blocking of State Route 530. The incident became known as the 'Oso Mudslide' or 'SR530 Landslide'. On April 3, the mudslide was declared a major disaster with loss estimates over $10 million. President Obama flew over the debris and met with survivors and families of victims on April 22. Search, rescue, and recovery efforts required extensive coordination among the local communities, the Snohomish County's Department of Emergency Management, the Washington State's Emergency Management Division (EMD) and FEMA. Resources were requested and tracked officially through WebEOC, but numerous other informal methods were used as well. The Washington Information Share Environment (WISE), an ArcGIS platform built by the Washington National Guard, was used to create a common operating picture (COP) among agencies using before and after imagery and geo-tagged data of the search and rescue findings.

2015 Washington Wildfires

The 2015 wildfire season was the largest in Washington State's history. Over 1 million acres were burned across the State between June and September. Over 3,000 Firefighters (including 1,500 National Guard members) were deployed in support of the firefighting effort. The resources of the Washington National Guard were requested by the WA State Emergency Operations Center (SEOC) and the WA Department of Natural Resources (DNR), through the WANG Joint Operations Center (JOC). Requested resources of the WANG included: hand crews, aviation, communication capabilities, security forces, and medical personnel. The JOC received official SEOC requests digitally via WebEOC and DNR requests digitally via DNR's Resource Ordering and Status System (ROSS).

Federal troops were requested by the National Interagency Fire Center (NIFC) through the Defense Support of Civil Authorities (DSCA) process and were assigned to fight fires.

2016 Cascadia Rising Rehearsal/Exercises

Cascadia Rising was a large scale, Federal/State multi-agency rehearsal/exercise of the Cascadia Subduction Zone catastrophic earthquake and tsunami response plan. The June 2016 rehearsal was a constructive (simulated), Command Post Exercise (CPX) and included linked full-scale exercises. The exercise rehearsed the plan of WA State, the WA National Guard, FEMA, USNORTHCOM (Department of Defense assets), and elements of Oregon and Idaho States. CR had several linked exercises incorporated into the base CR scenario, which included: Vigilant Guard (a WANG led domestic response exercise); Ardent Sentry (a USNORTHCOM Defense Support to Civil Authorities (DSCA) exercise); and Turbo Challenge (a USTRANSCOM logistics exercise). The primary focus of this exercise was to rehearse State/Federal support to WA State Counties.

In the WA Emergency Operations Center and in the WA National Guard JOC, WebEOC and WISE were primary systems used by participants. ROSS, described earlier, was not used as part of the exercise.

4.2.2 Interoperability Tools and Concepts

To support resource request and tracking in the context of emergent events, the broad regional community is guided by the overarching mission of achieving safety and security for affected populations. Large-scale emergent events inevitably involve multiple organizations in a collective effort to accomplish this mission. Information sharing among these organizations is essential. To the extent that the systems used by the varied organizations involved in these collective efforts can be made interoperable, they can ease the burden of information sharing.

Systems Supporting Resources Requests and Tracking in this Use Case

The key systems used to either request or track resources during these events were Washington State's WebEOC, the Washington Information Sharing Environment (WISE), and the Resource Ordering and Status System (ROSS).

WebEOC

http://mil.wa.gov/other-links/web-eoc

WebEOC® is software used within the Washington State Emergency Operations Center (EOC) as well as other local, state and federal EOCs. WebEOC is a web-based technology developed by Emergency Services integrators, Incorporated (ESi) for emergency management communications. WebEOC provides real time management of incidents with capabilities to conduct activities such as resource requesting and tracking, incident action plans (IAP), situation reports (SITREPS), and personnel management. The version of WebEOC used by the State of Washington is a public system and the information it contains regarding event management is public record.

FEMA also uses a separate instance of WebEOC for crisis management. The FEMA system is independent from the one utilized in WA. FEMA can and does grant non-FEMA individuals access to their instance of WebEOC. For example, individuals in the WA SEOC office have been given access to the FEMA WebEOC. The FEMA WebEOC is now a cloud-based system. Likewise, other instances of WebEOC, such as King County or City of Portland, are not automatically interoperable with others; each instance stands alone. Technically, the instances could be made to be interoperable, under different budgetary and policy conditions.

WA WebEOC is expected to upgrade to version 8 of WebEOC in the near future. Previous improvements were added to WebEOC based on recommendations from users and from lessons learned in after action reports, such as those related to the events discussed above. In the post-CR upgrade, the state's WebEOC will be moved to a cloud based system like the FEMA WebEOC.

The state's WebEOC Project Manager (PM) has worked with the WISE PM to share information. For example, if resource requests contain geo-locational data, these requests can be used by WISE to facilitate a GIS-based exploreable view. The state WebEOC operates as a stand-alone system with redundant back-ups in-case of outages, using phone, email, radio, fax and paper forms and submissions. In addition, these methods are always available for utilization by organizations that do not have Internet-based access to WebEOC. Because WA is a 'Home Rule State', the counties and cities cannot be mandated to utilize the system or to access it via the Internet.

WebEOC can push to WISE but it does not make sense to do so because there is no geo-tagged data in WebEOC. WebEOC is not currently designed to be interoperable with the other systems.

Washington Information Sharing Environment (WISE)

http://wise.mil.wa.gov/logtest/

The WISE is an ArcGIS platform created by the WANG to provide a common operating picture (COP) for the region. WISE was already in pilot form on December 9, 2009 when the Department of Homeland Security (DHS) announced the creation of Virtual USA (vUSA) as their flagship initiative to increase information sharing nationwide. At the time of the vUSA announcement, five states had formed the Pacific Northwest (PNW) vUSA Pilot, which included Alaska, Idaho, Montana, Oregon, and Washington.

Since its creation, WISE has undergone major improvements to allow for easier information sharing between agencies and states. Originally, WISE was only on an Army server and could not share information to users outside of that server. Recently, the current and third PM for WISE, created an "external facing" version on a public server in Olympia, WA in order to share unclassified information with the Air Force as well as regional agencies such as the WA Department of Transportation (WSDOT). For future development, the WANG is coordinating with Microsoft to transfer the server of WISE to an Azure Cloud platform for better performance and to ensure greater resilience for the region. Currently, the server in Olympia is susceptible to any regional catastrophic events.

The PM for WISE built an app for WebEOC on the Army server version of WISE. He also built apps that pull information from Twitter and YouTube regarding local incidents and is in the process of creating similar apps for the public server version of WISE. For access control and identity management, the PM grants access to users depending on their need to know and his recognition of their organization (ex: a WSDOT employee).

Access to the Army and Air Force sites are strictly controlled by CAC access and utilization of the system must be done from a .mil system. Information such as Blue Force Tracking is not automatically available on the public version of the site for security reasons. The Army site contains all data but the public site is filtered due to security and safety concerns. Each version of the system is unique and users must have separate login and access credentials for each of the systems.

WISE does not currently push data to WebEOC, nor does there appear to be a desire to do so. The WISE systems do have the ability to pull data that has geotagging (lat/long) information from the state WebEOC. Such interoperability is enabled by special arrangements between the WISE and state WebEOC administrators. Modules could be created to enable data-sharing between other systems like WebEOC and WISE, if there was sufficient funding and desire to do so.

WSDOT, Coast Guard District 13, some counties, and some local jurisdictions have access to accounts for using it. WANG would like WA State Patrol and the WA Department of Enterprise Services (DES) to use it as well.

Resource Ordering and Status System (ROSS)
http://famit.nwcg.gov/applications/ROSS

The National Interagency Resource Ordering and Status System (ROSS) operates in an estimated 400 interagency dispatch and coordination offices throughout the US. ROSS tracks all tactical, logistical, service and support resources mobilized by the incident dispatch community. In 1998, the National Wildfire Coordination Group (NWCG) chartered the ROSS Project to automate the manual resource status and ordering business process that primarily operated over telephones. ROSS operates under the guidance of the National Mobilization Guide and Dispatch Guides/Procedures. Policy is set by NWCG member agencies. The United States Forest Service (USFS) has been designated by the NWCG as the agency that is accountable for representing the interests of all NWCG member organizations. ROSS speeds the process and gives system users an enhanced understanding of:

- What quantity of resources are assigned to a fire;
- What quantity of resources are on the way to the fire;
- How deeply their resources have been depleted by requests;
- How soon local equipment will return from a distant assignment.

WA DNR subscribes to the ROSS system. According to DNR's ROSS managers, it is a highly useful and effective system. It has digitally automated their previous paper/phone call driven system. The Federal Government has approved ROSS to be used for "all hazards" as well as events (i.e., parades). ROSS is intended to be a multi-agency/interagency tool, designed to be used by users in various agencies (State and Federal) that are National Wildfire Coordination Group (NWCG) signatories. It feeds information into other compatible systems such as IQS, e-ISuite, and iRWIn. However, it is subject to some issues, such as firewalls blocking access to the program, and slow or no internet access impeding the functionality of ROSS. The ROSS server is centrally held in Kansas City. During the wildfires of 2015, the load on the ROSS server across the country was so great that it often crashed or needed to be taken off-line and rebooted.

The federal government requires each user of ROSS to agree to a federal security policy every year. ROSS can only be utilized for incidents, either planned or emergencies and users promise to not violate any applicable rules and laws. Agency personnel who are signatories to the National Wildland Coordinating Group (NWCG) use ROSS. Those agency personnel must submit their name, agency email address, agency and job title to the National Application Portal (NAP). Based upon this information, NAP personnel determine if access to ROSS is approved. If approved, ROSS can be downloaded onto a computer and a username and password will be emailed to the agency email address provided.

When resource requests originate in ROSS, they may be manually inputted into WISE. For example, during the wildfire event, WANG added information related to resource requests and tracking to WISE so that it could be part of the common operating picture (COP) in the JOC. WANG access to ROSS is granted to individuals in WANG on an as-needed basis. WANG has identified potential benefits to automating some information sharing with ROSS related to resource requests and tracking.

WA state EMD personnel can request access to ROSS, but have not needed to. Instead, communication between the state EMD and DNR representatives is conducted by telephone or email. A MOA between WANG and DNR approves ROSS requests to be sent directly to the WANG JOC and to bypass SEOC.

ROSS does not currently directly integrate or communicate with any other system. Participating States and agencies need to be granted access to the system to interact with it. Depending on current policies and applicable memorandums of agreement, a ROSS request for resourcing (from outside agencies) can either be sent to partnering States, EMD, or (if WANG centric) can be sent directly to the WANG JOC. For the wildfires of 2015, all ROSS requests were sent directly to the JOC. Given that WANG does not use ROSS, all ROSS requests are exported and delivered to the WANG via an email attachment. The user experience with the layout of data in this ROSS attachment is poor; WANG members have difficulty keeping track of annotated changes to specific requests during disaster response operations.

Tools and Concepts Supporting Resources Requests and Tracking in this Use Case

The following tables compare the three systems in this use case using the interoperability tools and concepts defined earlier in this report. These tools and concepts include access control, identity management, and NIEM (or similar data standards).

Table 3: Access Control Systems Used

Access Control			
	WebEOC	**WISE**	**ROSS**
	Handled by permissions system administered by WA State EOC. Access requests granted to individuals are assigned to an organization and group user level. System is accessed via a Web-based interface.	Request to current WISE PM, who grants either view, publish, or admin roles. Army version of this COP is more restricted than the state version of WISE. The state WISE is accessed via Web-based login.	Agency personnel who are signatories to the National Wildland Coordinating Group use ROSS. Those Agency personnel must submit their name, agency email address, agency and job title to NAP, the National Application Portal. Based upon this information, NAP personnel determine if they approve access to ROSS. If approved, ROSS can be downloaded onto a computer and a Username and Password will be emailed to the agency email address provided.

Table 4: Identity Management Systems Used

Identity Management			
	WebEOC	**WISE**	**ROSS**
	Identification is done by the PM, trusted sources	The WISE PM grants access upon request if	Agency personnel must submit their name, agency email

		person or email type is known. Username and password for WISE. System access can be enabled with accounts/passwords, but they can also use "tokens" that are location/person specific and thus not shareable	address, agency and job title to NAP, the National Application Portal. Based upon this information, NAP personnel determine if they approve access to ROSS. DNR Fire Dispatchers are the main users of ROSS. They must have ROSS access to create incidents and order resources. Train personnel in other sections of DNR that participate in a fire program and are interested in being Expanded Dispatch Recorders, Expanded Dispatch Support Dispatchers and Expanded Dispatch Supervisory Dispatchers. They must have ROSS rights to use the program.

Table 5: NIEM and Related Standards Used

NIEM			
	WebEOC	**WISE**	**ROSS**
	Not used	Not used	Not used

Additional Considerations Relevant to Interoperability in Systems Used to Support Resource Requests and Tracking

Organizational policies are a significant factor in the extent to which systems are made interoperable.

Table 6: Policy Constraints Towards Interoperability

Policy			
	WebEOC	**WISE**	**ROSS**
	Policy Constraint: 1. Home Rule State, use of Web EOC cannot be mandated	Policy Constraint: 1. The army's use of WISE includes personnel information.	1. To work properly, it requires the individual names / bumper numbers to equipment to be loaded into the system; this for

	2. Public Information, All information within WebEOC is public information and subject to FOIA 3. WebEOC is designated by the State for use in WA and is audited. (Ex: Seattle City Light has 1 or 2 people that use WebEOC, but info is transferred from Yammer) 4. Users are sometimes resistant to leave "paper trails" of resource requests 5. Some information cannot be shared easily (e.g., victim has a transmittable disease, possible bomb threat, etc)	This requires two versions of WISE – one for WANG and one for the State.	accounting purposes and reimbursement. 2. Federally mandated system with no flexibility for States to make adjustments. Slow process for States to recommend system changes. 3. Personnel/equipment are transferred during operations by ROSS changes of mission (however at the JOC level this is very confusing and not clear). 4. Some States will not provide assistance unless it's correctly filled out in ROSS. 5. The Federal Government has each person that uses ROSS agree to a Federal security policy every year. ROSS can only be utilized for incidents, either planned or emergencies and users promise to not violate any applicable rules and laws.

4.2.3 Tool Usefulness

Our research revealed other findings that are relevant to the technologies that support interoperability. Many of these observations are closely connected to the interoperability tools and concepts featured in this report. Some additional observations have secondary, contextual connections to core features of interoperability.

Observations Closely Aligned with Data Exchange Interoperability Tools and Concepts

Identity and Access Management

Access management is affected by the nature of the information in a system and prevailing laws/policies for access to that information. ICAM and IDAM for WISE and WebEOC are centrally controlled by the PM, excluding the full public access sites and the Army Site that requires CAC authentication and .mil access. Access control for the public WISE system and for the State WebEOC system is handled differently from many Department of Defense (DOD) systems because the information on these public/state systems is designated for use by citizen employees. Verification of personnel, roles and need for access are determined by the expertise of the PM and those who the PM trusts for verification. People who request access from official organizational email accounts such as a county.gov email address were considered to have a need to access the system.

In the context of emergency response, normal identity and access management tools may be loosened or discarded in order for people to focus on important mission-related work. In the context of the Cascadia Rising exercise, generic system user IDs and passwords were made available to all participants who needed to login to WA WebEOC or WISE so that they could focus on their work rather than system access. Additionally, in the exercise, EMD Logisticians would routinely input resource requests for others (i.e., local communities without WebEOC or those who could not access the system).

Improved identity management could lead to design changes that would improve the systems supporting mission-critical work in emergent events. During the Cascadia Rising exercise, for example, developers of the WISE system talked about the overpopulated map supporting their COP as the exercise was in progress. They noted that it would be helpful to create a system in which there would be layers of views depending on the identity of the user. They speculated that tying these layers of views to login credentials (which were not present during the exercise) would be desirable.

Exchange Patterns

Mission-based exchange patterns are complex, but improved capacity for information sharing may assist the community. For example, the WebEOC and ROSS systems do not communicate or have an ability to facilitate information sharing between each other. WA EMD receives assistance requests from State Agencies, Counties, Ports, and First Nation Tribes; then works to coordinate for other State assets to assist those requestors. Additionally, WA EMD has the ability to coordinate for assistance from other States via a system called the Emergency Management Agreement Compact (EMAC) Operating System (EMAC OS); this system also does not communicate or share information with WebEOC or ROSS. The EMAC OC can coordinate for other State's National Guard personnel and resources to assist in WA disaster recovery operations. Through the EMAC agreement, these other National Guard assets are attached to the WANG for operational control, then dispatched to specific incidents as related to standing ROSS and WebEOC requests. The lack of direct data sharing between the systems involved in these exchange patterns requires that humans be in the loop to achieve interoperability.

People engage in resource requests and allocation using outside systems. For example, as an EMD Logistician explained, *"We still have to take requests by phone due to not everyone having (WebEOC)."* That same EMD Logistician added, *"People with personal relationships* *circumvent the established system and bypass the mechanisms used to prevent redundancy."* A variation of this issue was offered by a deputy director of a county emergency management office, who observed, "*The game of authority (during emergency incidents) is like (the comedy sketch), 'Who's on first?'"* to explain why local leaders get frustrated and use backdoor channels to obtain resources, saying "*I don't trust (the official) process."*

The systems used by the broad community are tailored to the needs of the sponsoring organizations. For broader patterns of information sharing to emerge, configurations of what is shared would have to be highly customized. This point is illustrated in a quote from a representative of the WANG: *"The SEOC is kind of tracking what they have coordinated, but they're not very good at it... WebEOC is a data system. It's a problem and it requires constant upkeep and input. We, (the WANG), track our Soldiers for force protection, accountability, mission completion and compliance."* This observation was offered as the rationale for why the WANG uses their own systems for tracking. WebEOC, for them, is a requirement, not a useful tool (though it appears to work well for the WA SEOC and for FEMA).

When systems are not interoperable, people will modify their behaviors to do what is convenient to exchange information rather than to engage in more cumbersome technical work. For example, FEMA offers access to its version of WebEOC to approved WA SEOC personnel. However, according to a state EMD Emergency Logistician, *"If we need to request federal resources, we use the federal request form and upload each signed version to the SEOC and email it to our counterparts at FEMA. On rare occasions, we may logon to check the status, but have found that calling FEMA for the status of the request is the best use of our time."*

Lack of a requirement for people to use a system in an interoperable network of information sharing affects the exchange patterns in the network. For example, in the emergent situations considered, people were able to share information via means other than WebEOC, such as by using phone and/or email. In some instances, their information was entered into the system by others, creating a new exchange pattern and potentially having an effect on associating information with the identity of the information source.

The resource request form (RRF) is available to be filled out. The Requestor has the option to fax, email or call in the request to provide the information to the State EMD.

Data Standards

Lack of familiarity with a system affects how people use it, which may have consequences for interoperability. In the context of the Cascadia Rising exercise, many users had limited knowledge of WebEOC and consequently used only the simplest WebEOC features. In addition, their contributions to resources requests were often incomplete or misshapen. When such entries were viewed by others (so that the information would enable mission-based interoperability to be realized) the data had limited or no value.

The absence of a standard way of labeling data to be shared requires more humans to be involved in mission-based interoperability, where they must act as translators from one data-based system to another. For example, the WANG has friction in its work when synchronizing the daily reports of field-based managers with the tracking mechanisms utilized by the JOC, referenced to specific ROSS and WebEOC requests. This is a challenge because it requires an overly robust staff within the JOC to coalesce reports, perform data transformations, and backchannel reports into the WISE, SAD database, and accounting reports, during support of natural disaster response operations. The requirement for humans to be the bridge between the associated systems is a process gap in this important mission work.

Observations with Secondary Connections to Interoperability Tools and Concepts

Policy constraints affect interoperability more significantly than technical barriers. The PM for the state WebEOC system mentioned this when discussing why FEMA has a different version of WebEOC, which does not share information with the state versions of WebEOC. It requires States to do double work in some instances and monitor both systems, *"If there was no policy barrier we could technically connect today."*

Much of the system development work is conducted by a single (non-redundant) individual in the organizations. For example, the WISE PM for WANG explained, *"I'm not sure if (the WebEOC application for WISE) will be built for Cascadia Rising. The first overhaul is making sure (WISE) works on the AZURE clouds (in March), then (I'll) convert the older WebEOC application to JAVA script. (The WebEOC app) on the Army side is in FLEX."* Similarly, having only one or a handful of key experts on systems is a risk. As an EMD Logistician observed, *"A single point of success is also a single point of failure."*

4.2.4 Considerations for a Future Network of Interoperable Systems

Our investigation drew several conclusions for moving forward in developing interoperable systems in the future:

- Agreements about use need to be negotiated among stakeholders so that existing systems (e.g., instances of WebEOC) can be linked.
- To ensure data integrity and regular exchange patterns, training is needed to ensure more consistent, predictable use of systems.
- System-based error checking should be built into these systems to support data integrity and consistency. This error checking could leverage the potential value of NIEM and related standards.
- Identities of data contributors (sources of data) need to be handled more robustly and intelligently represented in the systems themselves.
- The multiplicity of systems needs to be examined and potentially reduced once greater interoperability is achieved.

4.3 Overview Across the Two Use Cases

The two use case studies in this report examine interoperability for information sharing in two notably different contexts: daily operations and disaster response. In this section of the report, we consider key similarities across the two cases identified in our investigation.

In both daily operations and disaster response, systems present in the work of the community are not structured and connected to be fully interoperable, nevertheless, people have found reasonable means of sharing information in support of accomplishing their work. Because people have found ways to get their work done in support of their organizational missions, there is not a widespread, explicitly perceived need to re-engineer systems or to redefine work practices. To prepare the community so that its members would perceive the need for and value of changes to their systems and work practices, the best approach may be to start with a community-facilitated analysis of pain points associated with their tools and practices, and to partner with members of the community in the co-design of improvements.

In both daily operations and disaster response, the existing ecology of systems and work practices present in the community is a workable, rational response to the laws, policies, and customs present in the region. The current state of interoperability in the Puget Sound region reflects the constraints that are well known to regional community players. Over time, the community has worked out information sharing practices and techniques that satisfy the demands of the community and are in compliance with relevant controls (e.g., Washington is a home-rule state; local and regional legal rulings about compliance with freedom of information laws).

In both daily operations and disaster response, budgetary considerations affect decisions to upgrade or re-engineer systems to support enhanced interoperability. Decisions about the systems that are used and the quality of those systems (newest versions of systems; modules included or absent) are frequently influenced by operating budgets for the organizations that must procure and sustain them. In several instances, the IT staff needed to support a system or the training staff needed to ensure consistent use of a system was surprisingly thin. The nature of systems (e.g., incorporation of optimal technical capabilities, robust user interface/experience design) as well as the education of the users has a direct consequence for the extent to which interoperability is realized in the work of the community.

The next section presents the results of additional qualitative analyses on use case data. These analyses shed additional light on regional interoperability issues and future ways forward.

5 Community Information Sharing and Safeguarding

An inherent tension exists when addressing the dual goals of simultaneously sharing critical information and safeguarding it. While increased transparency that results from information sharing provides mission benefits, trust and privacy concerns often outweigh these benefits. As we discovered during our work on MOISA, daily operational information sharing among the diverse set of regional agencies and stakeholders relied more on informal systems based on relationships and trust than on formal systems based on standards of identity and entitlement management.

The challenge to Project Interoperability is building increased interoperability into the largely informal trust-based systems that are already working well in the region. To help meet that challenge, a qualitative analysis was conducted on the data collected during the design and development of the planning and scheduling capabilities of IMDE/CSS (Use Case 1) and on the observations recorded at the Washington State EOC and the Washington National Guard JOC during the Cascadia Rising Exercise (Use Case 2). The sections below begin with a description of the qualitative analysis methodology, followed by the results and conclusions.

5.1 Qualitative Analysis of Interoperability

Content analysis is a qualitative research methodology used to interpret and code textual material with the intention of making valid inferences. Content analysis was used to address the foundational PIPS questions on PI tools as they applied in both the planning and scheduling of an interagency collaborative operation and a state-level disaster management exercise:

Questions: (1) How useful and applicable to mission accomplishment are these tools and concepts? (2) Why may these tools not be useful? (3) What strategies can be used to improve the design, usability, and outreach of these tools?

The first step in content analysis is to select the textual material to be analyzed. In the Planning and Scheduling use case, the textual material consisted of quantitative results from questionnaires as well as a summary of issues abstracted from open-ended survey questions and qualitative video and audio from the focus group and one-on-one design of the IMDE Planning and Scheduling field evaluation. For the Cascadia Rising Exercise, the textual materials were those observations documented by the project team members during the execution of the 4-day simulation.

The next step is to determine a meaningful categorization of the data. As our goal was to capture the important interoperability tools and concepts that applied in the two uses cases and identify opportunities for next generation tools, we created the following categories that reflected the four data exchange tools (see Section 3.1) and additional mission-centric tools: (1) Data Exchange for Identity and Access, (2) Data Exchange for Coordinated Operations, (3) Connectivity issues, (4) Coordination or issues related to mission compatibility and (5) Policy issues.

Interoperability concepts may be expressed implicitly as well as explicitly. While explicit terms are easy to identify, we expected to encounter very few explicit references. Coding for implicit terms is complicated by the subjective judgments of the human coders; therefore, we attempted to limit this subjectivity by using the following definitions for each concept:

1. **Data Exchange for Identity and Access Control.** This category includes the Attribute Exchange (tool 8) and Identity and Access Management (tool 7) data-centric interoperability tools. See Section 3.1 for a definition of these interoperability tools.
2. **Date Exchange for Coordinated Operations.** This category includes two additional data-centric interoperability tools: Exchange Patterns (tool 9) and NIEM standards (tool 10). See Section 3.1 for a definition of these interoperability tools.
3. **Connectivity Issues**. This category covers physical machine links and data pathways necessary to allow two systems to be connected to exchange information.
4. **Coordination or issues related to mission compatibility**. Coordination is the process of organizing people or groups so that they work together for mission accomplishment. For example, mission requirements within a local organization may be incompatible with the higher-level mission requirement of the state. This incompatibility results in poor coordination across the lower organizations for the accomplishment of the higher mission.
5. **Policy issues.** An instance where an existing policy affects interoperability for mission accomplishment or the instantiation of a new or modified policy that affects mission.

Coding was also complicated by the interdependent nature of interoperability. Information sharing requires more than just technical solutions; it requires partners to share trust that is built up over years of interaction as well as appropriate policies in place that guide or constrain these sharing relationships. As a result, the data that were coded often involved more than one interoperability concept and this is reflected in the analysis below.

5.1.1 Interagency Collaboration

To understand PI tools and concepts are applied in planning and scheduling of an interagency operation and to identify opportunities for mission-centric interoperability tools and concepts to support the information sharing necessary for planning and scheduling, data from the focus group and one-on-one design sessions of the planning and scheduling components of IMDE/CSS were used for the content analysis. These sessions resulted in 56 unique findings that were assigned to one or more of the interoperability categories described above. Nineteen findings were unrelated to interoperability (e.g., "*the app components menu is difficult to navigate. I am worried that if a user accidentally closes one of their widgets, they will not be able to find it again*"); therefore, they were removed from the analysis. In addition, due to the interdependent nature of the interoperability tools, some findings were placed in more than one category. The chart below provides a summary of the content analysis for the planning and scheduling use case data.

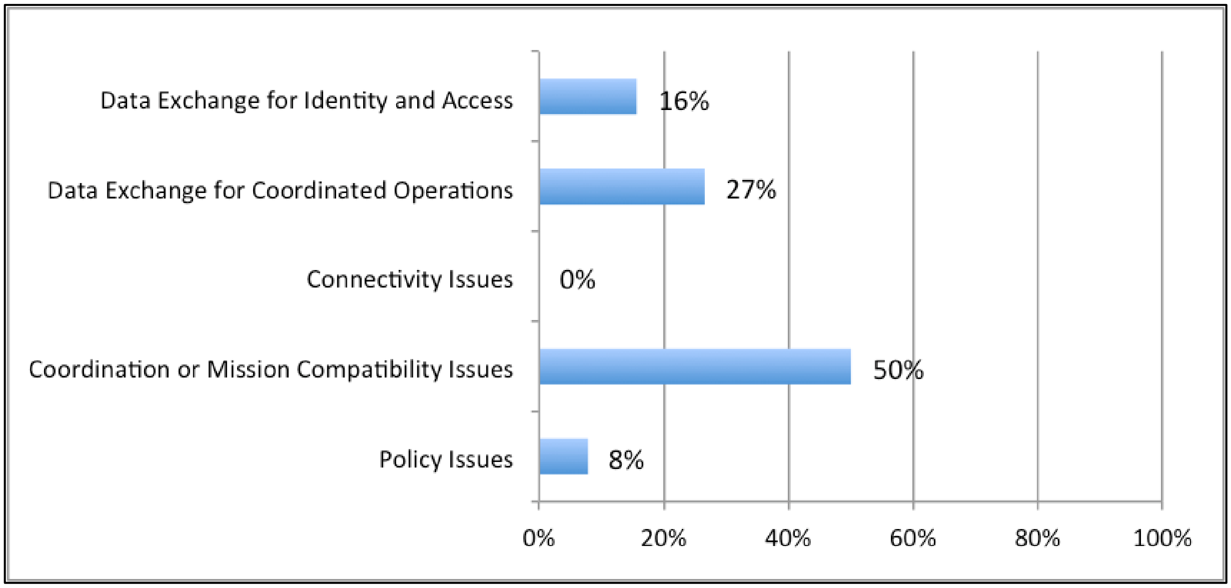


Figure 6: Content Analysis Summary for Planning and Scheduling Use Case

Forty-two percent of the findings were related to the two data-centric interoperability areas defined in Section 3.1. The interviewees did not explicitly mention the PI interoperability tools by name, but PIPS researchers coded design goals based on analysis of which tools, once fully developed, could help meet those goals. Below are examples of design goals that could be met through the use of one of the four data exchange interoperability tools: (Note: Connectivity was 0% in this analysis because IMDE was assumed to be providing those needs.)

Table 7: Interoperability Tool Improvement Challenges

Project Interoperability Tool	**Finding**
Attributes Exchange (tool 8)	It is also important that they have individual's qualifications in the system (referring to the need of LLE to assign crews to resources)
Identity and Access Management (tool 7)	Users have persistent sharing relationships, and thus selecting individual agencies to share with for each and every mission (as it is in the current design) would be prohibitively tedious.
Exchange patterns (tool 9)	Multiple users brought up the need for this system to pull/push data to and from MS Outlook.
NIEM (tool 10)	The way users enter date and time is problematic. Users need to be able to enter the time in military time without a colon.

Of the remaining findings, 58% presented opportunities for as yet to be developed mission-centric interoperability tools to address mission coordination issues (50%) or policy issues (8%). For example, "*users want the ability to filter by resources, by resource status, and by resource capability*;" thereby providing a feature that would allow each individual agency to view their resources in the way that would best serve their mission. Finally there were some opportunities for mission-centric tools that addressed policy issues. For example, the observation below appears to require a technical solution (e.g., improve the calendar interface to display more sharing agencies); however, the issue may in fact be better addressed by a mission-centric interoperability tool that incorporates policies that govern sharing relationships.

> *"Users will often want to share with many more agencies than can be displayed across the bottom of the calendar interface, so there needs to be a better way to display who they are sharing with based on their persistent sharing profile and/or the "share with" filter criteria they have selected."*

While the analysis reported above involved only the findings from the initial evaluations of the IMDE/CSS Planning and Scheduling Use Case and further development of this module is continuing, we can already see that interoperability tools, if developed further and extended into mission-based "gold tools," can be used to facilitate the exchange of information. In particular, this analysis reveals the need for further design and development of mission-centric interoperability tools such as the Information Sharing Matrix.

5.1.2 State-level Disaster Management

Content analysis was also conducted using the detailed observations collected by researchers embedded in the Cascadia Rising Exercise held on 4 – 7 June, 2016. The participants were located in the Washington State Emergency Operations Center and in the Washington National Guard Joint Operations Center. The majority of the observations concerned how the participants in these locations shared information with other participants throughout the Puget Sound region. Observers paid particular attention to the use of three systems: 1) Washington State's WebEOC, 2) the Washington Information Sharing Environment (WISE) and 3) the Resource Ordering and Status System (ROSS). See Section 4.2 for details concerning the Exercise and additional details concerning the three systems.

Many of the observations collected during the Cascadia Rising Exercised concerned logistical details about the actual exercise (e.g., 2 refueling spots in the region will be turned into fuel farms as more fuel arrives for aircraft), and as such were not included in the content analysis. The chart below provides a summary of the content analysis for the resource request and tracking use case. Note that some findings were coded using more than one of the categories listed above. The chart below provides a summary of the content analysis for this use case.

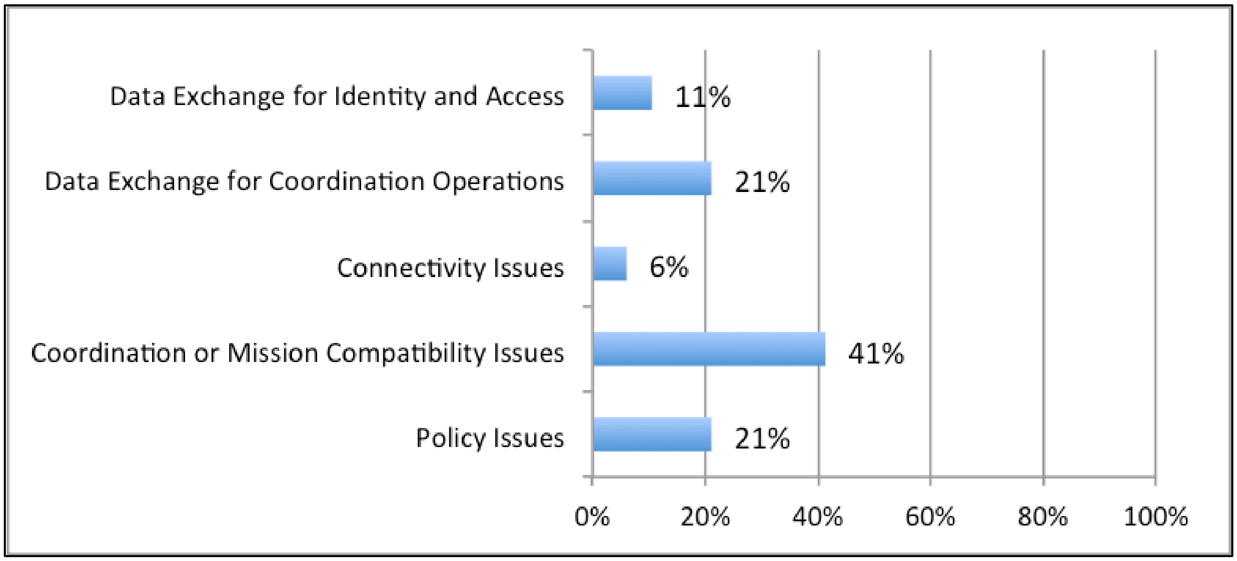


Figure 7: Content Analysis Summary for Resource Request and Tracking Use Case

Thirty-two percent of the findings were categorized as data-centric interoperability, with 11% belonging to Data Exchange for Identity and Access. Many identity and access rules were relaxed during the exercise in order to carry out the functions that are required. For example, generic system user IDs and passwords were made available to all participants who needed to login to WA WebEOC or WISE so that they could focus on their tasks. Problems arose because these generic IDs did not include source identity, resulting in a problem that can be seen in this example:

> *"WISE Is completely open. Users are anonymous they don't know who input the information because on the update whomever did it, didn't input their identity."*

It is not yet clear whether the relaxation of IdAM procedures is a feature of emergent emergency situations or of the exercise.

Other interoperability issues related to identity and access prevented responders from sharing needed information. For example,

> *"State and Army National Guard are running two systems - the State EOC computer and the Army computer (GKO) with CAD login. The State Guard does not have CAC cards; therefore they are unable to log into the Army site."*

Much of the information that was shared during the Cascadia Rising Exercise occurred outside of any of the three system discussed above; resulting in data exchange patterns that involved a human in the loop to achieve interoperability. For example, "*if a county is not up on WebEOC, the State EOC will take requests over the phone."* Much of the information exchange that occurred during Cascadia Rising was done over the phone or via email rather than system-to-system.

As stated in Section 4, lack of familiarity with a system affects how people use it (e.g., *Individual users are able to input information into WISE, but as I observed and stated yesterday, the users are not putting in all needed information, creating more work for the WISE developer)*. In the Cascadia Rising Exercise it not only affected how, but if the system was used. For example, *"Others who have sat at the WISE desk have not known how to do things with the system nor have they really attempted to actively do anything else with it."* Where emergency procedures related to ICS require people to use new systems in new ways, lack of training becomes a crucial issue.

Unlike in the Planning and Scheduling use case, we saw connectivity issues. This, of course, is due to the nature of the simulation. There were several times during the simulation when Internet access was not available, resulting in connectivity issues. In the Planning and Scheduling use case, it was assumed that all connectivity was handled by IMDE. During times when connectivity was unavailable, activity was significantly diminished as responders made due with radios and went back to their computers when connectivity was restored.

The majority of the observations (62%) were categorized under Coordination or mission compatibility (41%) or Policy issues (21%). As with the Planning and Scheduling Use Case, coordination and policy issues affected interoperability more significantly than the technical issues. Once again this demonstrates the need for further design and development of mission-centric interoperability tools such as the Information Sharing Matrix. The matrix, in particular, could provide a valuable framework for transferring trust in a dynamic environment such as disaster management where responders must go outside their usual trusted networks to gather and share information.

5.2 Qualitative Study Conclusions

The qualitative analysis revealed that there were very few explicit references to the four data exchange interoperability tools in either Use Case. This is not surprising given that these tools do not yet provide a well-defined solution to either identity and access management or data exchange. However, as the number of implicit references identified in these areas suggests, there is an opportunity for these tools to have an impact. Furthermore, the qualitative analysis revealed that data-centric tools have more impact in the case of daily operations than disaster management, suggesting that development efforts should focus on data exchange and IdAM use in daily operations. Partnering with community members in the co-design of these data-centric tools is essential to their acceptance and widespread use.

Finally, the qualitative analysis confirmed that the current PI tool set should include tools to address the mission-oriented interoperability layer. Tools are needed to facilitate community building, enhance coordinated operations, and incorporate the policy and legal requirements necessary for information sharing and safeguarding. The Information Sharing Matrix is a framework for capturing the existing trust relationships that could be used in the design and development of an identity and entitlement management component in an enterprise architecture like IMDE/CSS. A trust-based IdAM mechanism or system has the potential to not only provide the ability "to share the right information, with the right people, at the right time," but also to "strengthen safeguarding practices."[40]

[40] *National Strategy for Information Sharing and Safeguarding*, December 2012.

6 A Plan of Action for Moving Forward

PIPS found that from a regional perspective, Project Interoperability, and Federal interoperability efforts in general, need to shift focus from "bottom up" machine and data standards to "top down" issues of mission, policy, and organization. This is not to say that bottom up standards efforts are not important and necessary – they are. But they only become necessary after the top down issues are addressed in the only way they can be – in a partnership with the regional stakeholders. Once the regional partnership has clarified the information sharing benefits to missions; once they have identified and addressed potential unintended negative impacts; once they have integrated their policy and legal issues into the technology innovation; in short, once the regional community has taken ownership of an interoperability innovation and articulated what they want and how they are willing to work collaboratively to make it happen, then the machine and data standards will become vital tools for making it happen. But without solving these higher level issues first, the lower level ones will sit there like hammers looking for a nail.

One reason that PM-ISE funded the University of Washington to conduct PIPS was its role as a collaborator in the regional security and public safety community (e.g. as a member of the Area Maritime Security Committee). A goal of PIPS has been to engage CoSSaR as a facilitator in regional efforts to enhance security and public safety through increased interoperability and information sharing. Following is a plan of action and milestones, focusing on the role CoSSaR can play in accomplishing this goal:

1. Move Project Interoperability initiatives higher up the "interoperability continuum," that is, more towards community partnerships to co-develop and demonstrate mission-based tools and concepts.

   a. CoSSaR, working with PM-ISE, engages with Project Interoperability to initiate the addition of mission and community focused "gold tools" to the PI toolset, beginning perhaps with the matrix, trust-based IdAM concept introduced in Section 3.2, or a functional language of policy expression as discussed under Attribute Exchange in 3.1.4.
   Timeframe: Primary engagement at the WIS$_3$ meeting on March 23, 2017 in Reston VA.
   Milestone: A new PI "gold tools" initiative.

   b. CoSSaR engages with Puget Sound stakeholders in the operational community to participate in a PI "gold tools" initiative, focused around enhancements identified by the community as desirable such as a digital interagency IAP (Section 4.1.2).
   Timeframe: January – December 2017
   Milestone: A regional stakeholder partnership with PI.

c. CoSSaR, with PM-ISE, Coast Guard IOC, and NMIO, continues work with DHS S&T on IMDE/CSS modules (or future Apex modules) employing human-centered design, development and implementation methodologies for co-creation with the regional community.
Timeframe: January 2017 – December 2018
Milestone: Implementation of module(s) delivered through the IMDE enterprise architecture and being used by regional stakeholders to enhance their security and public safety missions.

2. Address the need for community outreach regarding achieving interoperability by establishing CoSSaR as a regional resource for operational interoperability innovation. This can become a model for other regions to follow to facilitate interoperability. Puget Sound is uniquely positioned to establish such a model.

a. Establish a regional interoperability and information sharing laboratory, where partner stakeholders can come together and explore mission-based interoperability initiatives facilitated by experts, using state-of-the-art tools, strategies and resources. Establish linkages to related facilities, such as the new Post-Disaster, Rapid Response Research Facility (RAPID) funded by a $4.1 million National Science Foundation grant.[41]
Timeframe: January – December 2017
Milestone: The Interoperability and Information Sharing Laboratory (The IIS Lab) is open and supporting collaborative projects to enhance mission accomplishment through improved system interoperability and mission-based information sharing. The IIS Lab is also developing reusable information sharing "modules" and reaching out to help adapt them to other regions.

b. Establish an online Interoperability Information Resource (IIR) to provide information, answer questions, and link operational agencies to resources for enhancing mission through improved system interoperability.
Timeframe: January – June 2017
Milestone: The IIR operational by summer of 2017

3. Enhance Federal and regional interoperability initiatives by incorporating human-centered design and development strategies and methodologies that foster co-created, agile, mission-based, iterative design and development of operational interoperability innovations.

a. Engage with regional operational stakeholders to socialize human-centered strategies and explore how those strategies can empower them to guide the selection of

[41] RAPID is part of a recent $19 million investment by the NSF's Natural Hazards Engineering Research Infrastructure program.

interoperability issues to be addressed and innovations to address those issues. The overall goal is to enable regional co-creation of the future Puget Sound information sharing environment.
Timeframe: January – June 2017
Milestone: A regional structure, perhaps under the Area Maritime Security Committee, that fosters regional stakeholder partnerships supporting human-centered interoperability initiatives.

b. Work with Federal entities such as PM-ISE and 18F[42] to engage Federal sponsors of regional interoperability initiatives and facilitate their adoption of human-centered strategies and methodologies, and to partner them with regional stakeholders to implement those strategies and methodologies.
Timeframe: January – December 2017
Milestone: A Federal interoperability project partnered with regional stakeholders to achieve innovation by employing human centered design and development strategies and methodologies.

This POAM presents seven project activities under three overarching areas: (1) Moving Federal interoperability initiatives higher up the interoperability continuum; (2) Serving regional interoperability needs for information and guidance; and (3) Employing human- centered, agile methodologies to achieve interoperability objectives. Through these initiatives, CoSSaR will partner with regional operational stakeholders, Federal interoperability leaders, and interoperability experts and researchers from academia and industry to move national interoperability efforts towards more mission-based, community-centered design, development, implementation and evolution. As documented in this report, this movement is crucial for the success of our nation's program to promote innovation aimed at achieving appropriate and effective information sharing and safeguarding.

[42] 18F is housed in GSA with the mission to "build world-class digital services" using "human-centered design, agile methodologies, and open source software," https://18f.gsa.gov/ accessed 10/12/2016.