REGIONAL RESILIENCE AND THE INFORMATION SHARING ENVIRONMENT

CoSSaR White Paper #1
Prepared for FEMA's 2015 Annual Mitigation Summit
Seattle, WA

Center for Collaborative Systems for
Security, Safety, and Regional Resilience
cossar@uw.edu
hcde.uw.edu/cossar

HCDE Human Centered Design & Engineering

COLLEGE OF ENGINEERING
UNIVERSITY of WASHINGTON

This white paper is adapted from the Year One Report of the Maritime Operational Information Sharing Analysis (MOISA 1) project.

CoSSaR acknowledges the contributions made to the research and publication of the Maritime Operational Information Sharing Analysis Report. We would like to thank the Puget Sound Maritime Community for their continued support throughout the project, especially the 77 individuals from 52 organizations who contributed their time and expertise.

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

We would also like to thank the sponsors for their support and contributions as partners in this project.
• Department of Homeland Security Interagency Operation Centers Program
• National Maritime Intelligence-Integration Office
• Program Manager for the Information Sharing Environment

CoSSaR contributors:

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

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

Consultants:
Christena Little and Anne Tyler

Principal Investigators:
Dr. Keith Butler, Dr. Mark Haselkorn, and Dr. Mark Zachry

Resilience is often thought of in terms of the economy or infrastructure, but recent work by CoSSaR researchers has highlighted the critical connection between regional resilience and information sharing. The strength and effectiveness of the regional information sharing environment (ISE) is a critical and often overlooked component of regional resilience.

Post-9/11, our Nation's security strategy has focused on inter-agency coordination and information sharing in the context of major incidents. Through a massive effort we have established the National Incident Management System (NIMS) which provides incident management standards of operation that enhance our nation's ability to coordinate responder activities. But security and safety are not just incident-based endeavors; they are also services that must, like power and transportation, be operational 24/7 in support of economic resilience and societal well-being. Now a comparable NIMS-like effort is needed, but focused on daily multi-agency operational information sharing and coordination.

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

Year one of the Maritime Operational Information Sharing Analysis (MOISA1) project was a collaborative effort with the Puget Sound safety and security community (PSSSC) to answer the question: What is the nature of the PSSSC's daily operational ISE and what is the role of that ISE in achieving their collective missions? The community's answer, repeated many times in

[1] NMIO website, http://nmio.ise.gov/
[2] PM-ISE website, http://www.ise.gov/mission-and-vision

many ways, was simple and nearly unanimous: "When it comes down to it, it is all about relationships."

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

The ISE of daily operations is not the same as the ISE of incident response. We found that most members of the community do not on a daily basis see security as their job one. Even a police interviewee identified his primary job as community relations. Daily operations occur at a different pace and focus than the intensity and time pressure of incident response. Daily operations are highly impacted by economics, one of many barriers to information sharing due to competition; barriers that are set aside during incident response. Yet despite these and other differences, the ISEs of daily operations and incident response are intimately intertwined. While the PSSSC works hard to strengthen its relationship-based operational ISE, there are still some critical gaps. There are gaps from personnel turnover and retirement, from stove-piped thinking and investment, from conflicting priorities and missions and cultures. Where gaps exist, regional resilience is decreased. Gaps in the community fabric of trust and self-knowledge; gaps in the framework for information sharing; gaps in the understanding of who needs what, when, how and whether or not they should receive it; these translate into less effective and responsive action by the community. For this reason, the PSSSC invests significant time and energy in an ongoing effort to establish trusted relationships and achieve self-knowledge.

There are numerous formal systems in the Puget Sound region, most developed with Federal investment, intended to enhance the way the PSSSC receives, stores, and shares incident-focused information. While the maritime community's focus on trust relationships, and the ability of these relationships to support highly nuanced information sharing, may sound unrelated to these often state-of-the-art technology-based security initiatives, these initiatives wrestle with the same issues of trust and information access. Furthermore, these technology "solutions" are dependent upon acceptance and use within the community's operational ISE for sustained existence and meaningful impact.

The parts of these technology-based information and communication systems that come closest to acknowledging the daily operational ISE work of the community are identity and entitlement management – who are you, can I trust you, what can I appropriately share with you? In terms of systems design, formal methods for identity and entitlement management are a major focus of national initiatives to improve the ISE, but thus far these formal methods are far less of a focus of the diverse regional community. The PSSSC shows little interest in or awareness of data standards or meta-tagging or national exchange models. Perhaps this is because they are working on a daily basis to maintain a nuanced and often non-technology based system of identity, entitlement and trust management, focused on knowledge of and experience with people, organizations and work practices.

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

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

There are critical questions to be answered. What will it take to align Federal investment in security and safety with regional work and practices to better achieve that security and safety for its citizens, institutions, and infrastructure? What will it take to achieve community acceptance and ownership of future solutions and strategies? How do we design sustainable solutions and strategies that improve over time and with use, rather than degrade as they currently do?
In order for Federal investments in formal systems to meaningfully impact regional resilience, these systems must be designed and implemented through methods that center on humans and their work. Throughout the life-cycle of technology systems intended to enhance the regional ISE, designers, developers and sponsors need to work closely with the regional operations community to address the informal aspects of actual work as well as the formal assumptions of policy and procedure, the diverse daily operational environment as well as the centrally structured NIMS environment, the human and work needs as well as the technological constraints.

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