Appendix H
2009 MIST (Puget Sound)
Executive Summary

Executive Summary

This report presents the findings of the Maritime Information Sharing Taskforce (MIST) research effort for the Washington State Puget Sound ports. Using a participatory design approach, the researchers partnered with federal and commercial stakeholders to assess the information sharing needs of security personnel in this port region. The research design included an issues workshop, field studies of port personnel, and local networking events. The findings indicate the need for increased interagency collaboration in maritime domain awareness (MDA) and highlight local recommended practices and incentives for information sharing with the private sector. In addition, we gathered usability data on two federal policies/programs.

About MIST

The Maritime Information Sharing Taskforce (MIST) is an interagency effort to capture best practices in information sharing, create a structure for collaborative problem solving, and convey unique local issues to national policy makers. The MIST team is led by the Maritime Defense and Security Research Program (MDSRP) at the Naval Postgraduate School (NPS) in partnership with several federal agencies: the Maritime Administration (MARAD), the Office of Global Maritime Situational Awareness (OGMSA), Global Maritime and Air Intelligence Integration (GMAII), the U.S. Coast Guard (USCG), Customs and Border Protection (CBP), and Naval Cooperation and Guidance for Shipping (NCAGS).

The MIST process consists of a series of activities that are designed to help us surface issues important to private sector shipping. Each local event builds upon lessons learned from earlier events and invites participants to join in on the design of specific activities. Figure 1 shows the six steps of the MIST process. Steps one and two are base line activities and were used at our prototype event at the Ports of Los Angeles and Long Beach and at our most recent event at the Ports of Puget Sound. The primary activity (1) is a local workshop that is designed to uncover key issues surrounding the sharing of threat information. This activity is supported by a social networking website (2) that allows participants to respond to weekly polls, interact with each other, and share maritime security resources. Based on the findings from our first workshop, we expanded our community bridging activities (3) for Puget Sound to include a pre-workshop reception and on-going email polling. To help us better understand daily practices, we also added in field studies that looked at real world information sharing behaviors (4). Finally, to help us build a better understanding of the information sharing needs of the private sector, our future plans include the development of network relationship maps (5) and a national feedback mechanism to assess private sector needs (6). Each MIST activity is participatory in nature and invites federal agencies and local private sector communities to join in the design and execution of the activities.

Figure 1: the MIST Process

Executive Summary

Our findings

During our work with Puget Sound ports, we focused on three main goals:

1. Identify local issues, recommended activities, and key incentives for information sharing
2. Identify local practices and resources used in information sharing
3. Analyze selected federal policies for desirability, effectiveness, and ease of use

Following is a high level discussion of our findings. These findings are further detailed in the full report.

The Puget Sound is driven by economics and safety

As in LA/LB, the Puget Sound participants identified financial benefits and operational efficiencies as the most important incentives for information sharing. In addition, they identified secondary strategic and social benefits.

Financial and Operational Incentives

Puget Sound participants acknowledged the importance of information sharing to its financial and operational concerns: "economic and social efficiency is maximized through transparency and information sharing." However, the participants also discussed how the current economic downturn will negatively impact its security efforts. They emphasized the importance of resource sharing and pointed out how economic pressures may lead them to focus more on the intent of rules over strict compliance. Upcoming budget decreases, combined with pressures from labor, will also most likely lead to a re-emphasis on safety issues. Finally, participants tied their need for predictable requirements into effective decision-making and business planning activities.

Puget Sound participants, like their LA/LB counterparts, identified fewer delays, faster throughput of goods, and faster ship turn around as key outcomes. In addition, the Puget Sound highlighted specific effects measures related to emergency management—more effective drills, more robust preparedness levels, and a decline in user complaints.

Profile of an FSO[1]
(Facilities Security Officer)
Background and Goals

John is only one of the over 200,000 people working in the ports of Washington state, and he, like many facility security officers, has a unique background. Some FSO's are military or police trained, and some like John have come up from operations; some have college degrees and some have learned on the docks. Almost all FSO's have spent a good deal of time in the maritime industry and are dedicated to keeping their facilities safe. Though, at 43 with a family and kids, John has to work hard at balancing work demands and time with his family.

John does safety, security and operations

As the safety officer for a container shipping company, John saw his job expand to security officer after 9-11. New regulations meant he had to take specific training with the U.S. Coast Guard (USCG) and assume new responsibilities for security. His day-to-day job includes managing access to the facility, doing vulnerability assessments, assessing environmental impacts, implementing technologies, and handling insurance and regulatory issues for his company. He has to deal with all the security related programs—federal reports and mandates, fire regulations, and drills. Now, with the economic downturn, it looks like his duties will change again to include more oversight of yard, rail, and ship activities, mechanical repairs, labor relations, and project management. Like everyone else in his company, John is **"here to make money and we facilitate that."**

1 *The profile of John in the sidebar is a synthesis of data collected from four on-site interviews with facility security officers in the Puget Sound area. John is not a real person but is an archetype that can be used to better understand the needs and goals of security officers. The profile has been submitted to active facility security officers to validate the general descriptions presented here.*

Executive Summary

Strategic Incentives
Participants in the Puget Sound noted the strategic benefits of information sharing. When a threat is well understood, security professionals can more easily justify security expenditures to management, customers, and public stakeholders—"I can tell them what the money is for." Better information sharing also helps improve collaboration during grant writing and during emergency drills. In addition, information partnerships can be a strategic advantage for smaller ports by expanding and strengthening their voice.

Social Incentives
Finally, participants identified trust, workplace satisfaction, and strong communities as key social benefits of information sharing. Quality information sharing can increase trust between industry and the government and between industry and labor. Actionable threat information can also help security professionals better plan, execute, and communicate their security responsibilities, thereby improving workplace satisfaction and management buy-in. And, information sharing can create feelings of inclusion and interconnectedness for those new to the community.

Recommendations
1. Address the impacts of the economic downturn
2. Align policies and procedures with economic concerns
3. Minimize regulatory barriers
4. Incentivize resource sharing
5. Phase implementations to increase predictability
6. Align and empower strategic partners
7. Support local efforts in community building – *bridge, don't build*
8. Directly address union concerns
9. Align strategic security communication efforts with safety concerns

Local interagency collaboration is strong, but stove-piping is a problem

When asked about areas where government could be streamlined, the Puget Sound participants identified the need for improved interagency collaboration and less stove-piping.

In the Puget Sound, although there were challenges with dealing with federal agencies in general, participants were mostly satisfied with the interagency collaboration of their two main federal partners—the U.S. Coast Guard (USCG) and Customs and Border Protection (CBP). Participants saw the two agencies as being less stove piped and better coordinated at the local level than is typical; for example, in coordinating boarding activities, collaborating on the mitigation of environmental threats, and doing combined exercises. The local Area Maritime Security Committee (AMSC) is seen as a strong organization due to its intermodal point of view and its integration of facilities, infrastructure, and vessel security. In addition, the local AMSC integrates information technologies and law enforcement agencies, and effectively uses subcommittees – especially the Facility Security Officer (FSO) Subcommittee.

Executive Summary

Participants did note that *federal* stove-piping tended to impede communication and prevent the creation of a "one-stop place" for information sharing. This stove-piping impacts federal regulations, resulting in cross agency differences in information technology (IT) policies, overly complex programs and procedures, and conflicts between regulations and private sector business rules.

Recommendations

10. Utilize an effects-based[2] approach to maritime strategy that includes private sector input
11. Increase institutional support for interagency collaboration
12. Conduct customer service audits
13. Increase support for face-to-face communications
14. Allow flexibility on unfunded mandates
15. Align regulations with business rules and practices

Good communication is key

Puget Sound participants want quality communications, a single point of contact for threat information, and want to communicate across boundaries.

First and foremost, participants noted the lack of access to threat information. Participants do not receive regular threat information and feel that information sharing is a one-way street. Security professionals need a single point of contact for both reporting and receiving threat information and they want good customer service. Participants wanted the federal government to facilitate a system that "brings stakeholders together, validates concerns, and gives directions and procedures", but does not take over local control. Participants felt that it is also important to utilize waterfront residents "as your eyes and ears."

Secondly, Puget Sound participants necessarily interact with a wide range of communities and a potential role for the federal government is to ease communication with these communities. The agencies cross international, federal, state, tribal, and local boundaries and each serves a unique function. Puget Sound participants identified the importance of using a variety of communication modes—face-to-face, web, emails, and newsletters—to help bridge functional and local needs, to leverage the local workforce, to increase networking and to build trust.

Recommendations

16. Utilize an effects-based[2] approach to maritime strategy that includes private sector input

[2] *An effects-based approach determines actions and policies based on the desired outcomes of stakeholders*

Profile of an FSO
Information needs

John values personal communication
In his daily work, John interfaces with a lot of people and agencies – management, employees, vendors, labor, port authorities, the USCG, Customs and Border Patrol (CBP), Harbor Patrol, Police and Fire, and a slew of state and federal agencies. Sometimes communication is tough when the government side rotates so often—the private sector has to keep training them and there's no continuity. Things really don't work for John if he doesn't have a good personal relationship with these folks. In the office, he uses email and the phone. In the yard the radio is key, and everywhere, the cell phone is a must have.

John needs info pushed down to him
From arriving in the morning to mid - day checks to middle of the night calls, John's job is making sure the place is locked up and everyone is safe. When it comes to knowing what's up, John doesn't have time to go out and dig for information. He needs all hazard information sent to him. He needs to know if there are emergency situations or international threats, local law enforcement threats or threats from druggies and people who just have an axe to grind. If there is no threat, his company needs to know that as well, so they can refocus on making money.

John wants info tailored to his needs
There are existing resources that are helping John stay informed. The USCG relationship and AMSC are good. AIS data and the FSO committee are invaluable. The Joint Harbor Operations Center (JHOC) concept is solid. HOMEPORT alerts, USCG emails, traffic and weather alerts, and some of the independent blog dailies like NW Warn are useful, but there are just "too damn many of them." Email has been good but it would be nice if there was a better way to do common postings that are specific to his region and needs. And, John would be really happy if he could destroy government silos, get over the pain of security filters, and just get everybody working better with the ground forces.

Executive Summary

- *Support local networking and include a diversity of roles, ports, and functions*
- *Connect regional partners with state and federal agencies*
- *Coordinate federal MDA activities, resources, and data*
- *Manage a central reporting system and integrate it with a central sharing system*

Information should be easy to access and of high quality

Puget Sound participants explored the characteristics of an "ideal" information system and identified key characteristics and barriers in using information systems.

One of the key initial barriers to information sharing is getting access to the information. First, password policies should not be a barrier. Second, Puget Sound participants, like their LA/LB counterparts, want a central repository for information and need that system to be easy to access. Easy access includes information that is "centrally located", "pushed to me" and accessible "anytime, anywhere." In addition, when looking at a proposed new information system, we discovered the importance of aligning the system with internal processes. For instance, in the case presented, we discovered that internal communication policies of the private sector did not align with the proposed communication process for an international information number (see p. 17 *Dial "S-E-A"* sidebar for more details).

The way in which information is presented is also important. Information should be presented in such a way that it shows trends and provides "real-time, actionable, self-correcting data." It should be easy to understand – using "simple language" topic driven menus, and utilizing "executive summaries with supporting data behind." As an example, participants reviewed HOMEPORT during the workshop and found that its menu structure and overall organization made it difficult to get to needed information (see p. 21 *HOMEPORT* sidebar for more details).

Participants also helped us define the characteristics of "ideal" information. For Puget Sound participants, the information should above all be relevant: "customizable to my interests", "regionally targeted", and "show functional impacts" such as the impact on the cargo flow. Systems should utilize "premade profiles based on communities of interest." And most important of all, participants want access to relevant classified information so they can make informed decisions. Participants conveyed they expect this level of access may help them "know whether the threats we are having are homegrown terrorists or international cells."

Recommendations

17. Improve access to MDA information (push data to the private sector, scrub classified data, allow anytime/anywhere access)
18. Provide information that is needed by commercial sector (all hazard, situational awareness, financial /operational impacts, neighborhood alerts, resources)
19. Ensure high quality data (regionally targeted, up-to-date and synchronized, intermodal, actionable, relevant)
20. Ensure usable information (trustworthy, accurate, complete, simple, most important first, based on "communities of interests" and topic driven

MIST should provide value and be sustainable

After holding two MIST events, the value of including local commercial input into the MDA effort is clear. Our federal partners are receiving tangible information to inform their decision making, and participants rate the MIST events as very well organized and useful – 4 and 3.5 respectively on a 4 point scale. We are beginning to see trends across local ports and at the

Executive Summary

national level. Our move to more specific problem solving is providing us with more actionable data. And, we are continuing to identify a number of "best practices" and "hotspots" that can help improve MDA efforts.

To improve the effectiveness of MIST, we recommend several high level next steps:

Recommendations

17. Partner with a funded, empowered, and respected MDA agency that can provide continuity and on-going support to local efforts
18. Tailor MIST activities to provide value tothe public sector (e.g. to help with Port Security Grant applications)
19. Include a feedback mechanism that allows local particulars to be standardized and analyzed across ports (e.g. policy and technology evaluations, collaborative capacity assessments)
20. Include a network mapping process that identifies and describes the effectiveness of key relationships
25. Establish a sustainable funding model (repeatable, 2x yearly)
26. Continue to improve MIST internal processes

(The complete report is available at www.gmsa.gov/gmiss)