

MIST

Maritime Information Sharing Taskforce



Industry and Public Sector Cooperation for Information Sharing Ports of the Puget Sound

Anita Salem

Naval Postgraduate School

Wendy Walsh

Naval Postgraduate School

Lyla Englehorn

Naval Postgraduate School



July, 2009

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUL 2009		2. REPORT TYPE		3. DATES COVERED 00-00-2009 to 00-00-2009	
4. TITLE AND SUBTITLE Industry and Public Sector Cooperation for Information Sharing. Ports of the Puget Sound				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School, Operations Research Department, Monterey, CA, 93943				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 46	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Table of Contents

EXECUTIVE SUMMARY:

ABOUT MIST	3
-------------------------	----------

OUR FINDINGS.....	4
--------------------------	----------

THE PUGET SOUND IS DRIVEN BY ECONOMICS AND SAFETY	4
---	---

LOCAL INTERAGENCY COLLABORATION IS STRONG, BUT STOVE-PIPING IS A PROBLEM.....	5
---	---

GOOD COMMUNICATION IS KEY	6
---------------------------------	---

INFORMATION SHOULD BE EASY TO ACCESS AND OF HIGH QUALITY	7
--	---

MIST SHOULD PROVIDE VALUE AND BE SUSTAINABLE	7
--	---

PROFILE OF AN FSO.....	4 and 6
-------------------------------	----------------

INTRODUCTION:

ABSTRACT	8
-----------------------	----------

WHY MIST?.....	10
-----------------------	-----------

WHY THE PRIVATE SECTOR?	10
--------------------------------------	-----------

WHAT ARE OUR CHALLENGES?	11
---------------------------------------	-----------

FINDINGS:

INCENTIVES AND PERCEIVED BENEFITS.....	14
---	-----------

PERFORMANCE MEASURES THAT IMPACT THE BUSINESS OPERATION	17
--	-----------

STREAMLINING GOVERNMENT	17
--------------------------------------	-----------

INFORMATION FLOW.....	19
------------------------------	-----------

CASE STUDY: DIAL "S-E-A".....	17
--------------------------------------	-----------

CASE STUDY: SEATTLE AMSC.....	19
--------------------------------------	-----------

CASE STUDY: HOMEPORT.....	21
----------------------------------	-----------

LESSONS LEARNED:

THE WAY FORWARD	23
------------------------------	-----------

LESSONS LEARNED ABOUT MIST PROCESSES	23
---	-----------

APPENDICES:

APPENDIX A: METHODS.....	27
---------------------------------	-----------

APPENDIX B: SURVEY AND EVALUATION RESULTS.....	32
---	-----------

APPENDIX C: SURVEY AND EVALUATION INSTRUMENTS	38
--	-----------

APPENDIX D: LIST OF ACRONYMS	43
---	-----------

APPENDIX E: REFERENCES.....	45
------------------------------------	-----------

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.

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.



Profile of an FSO¹ (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.”

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-based² 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. Give a single agency the power and resources to support and enhance local communication:

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. HOMEPOR 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.



- *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

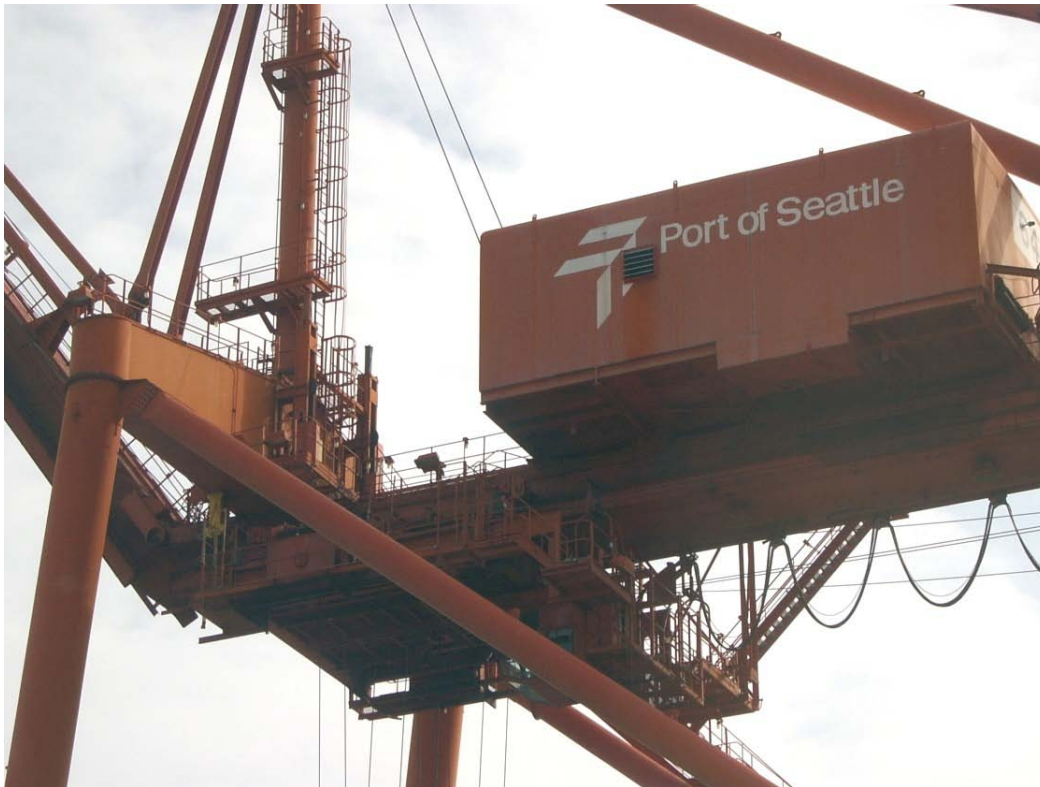
After holding two MIST events, the value of including local commercial input into the MDA effort is clear. Our federal partners are receiving tangible information to inform their decision making, and participants rate the MIST events as very well organized and useful – 4 and 3.5 respectively on a 4 point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

21. Partner with a funded, empowered, and respected MDA agency that can provide continuity and on-going support to local efforts
22. Tailor MIST activities to provide value to the public sector (e.g. to help with Port Security Grant applications)
23. Include a feedback mechanism that allows local particulars to be standardized and analyzed across ports (e.g. policy and technology evaluations, collaborative capacity assessments)
24. 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



Abstract

Following the terrorist attacks on the United States on September 11, 2001, the sharing of threat information between government agencies and the private shipping industry became a top priority. As initiatives progress, private industry is being asked to share more of what they know and yet is still provided with little or no reciprocal security information. The Maritime Information Sharing Taskforce (MIST) is an interagency effort to improve this situation by capturing best practices in information sharing, creating a structure for collaborative problem solving, and communicating unique local issues to national policy makers. Using problem solving workshops, polling, social networking, and field observations, the MIST process identifies local issues, activities, resources, and incentives for information sharing. Working directly with local stakeholders, MIST also explores the desirability, usefulness, and usability of new policies and technologies. Our findings indicate gaps in information sharing and collaboration, poor alignment of information systems with user needs, and the need for appropriate financial, operational, strategic, and social incentives for information sharing. Looking forward, we recommend continuing on-going input from local practitioners, funding community bridging efforts, and improving interagency collaboration.

Introduction

MIST is a two-way process for understanding and communicating the needs of local, private sector communities when sharing security information.

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 2 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 the Puget Sound. Activity (1), the local workshop, is our core activity and 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. We also added in field studies that looked at



Figure 2: the MIST Process

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.

Why MIST?

Driven by presidential and congressional mandates to share threat information following the terrorist attacks on the U.S. on September 11, 2001, the federal government established a series of policies and programs to integrate private sector input into national maritime security efforts. The Maritime Security Interagency Policy Coordinating Committee (MSIPCC), established with the release of Presidential Policy Directive 1 on February 13, 2009³ is the primary forum for coordinating U.S. government maritime security policies. The MSIPCC continues the intent of the National Security Presidential Directive 41 /Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13) which originally tasked this body to oversee the development of a National Strategy for Maritime Security (NSMS) with five named strategies and eight supporting implementation plans:

STRATEGIES	SUPPORTING IMPLEMENTATION PLANS
1. Enhance International Cooperation	1. National Plan to Achieve Domain Awareness
2. Maximize Domain Awareness	2. Global Maritime Intelligence Integration Plan
3. Embed Security into Commercial Practices	3. Interim Maritime Operational Threat Response Plan
4. Deploy Layered Security	4. International Outreach and Coordination Strategy
5. Assure Continuity of the Marine Transportation System	5. Maritime Infrastructure Recovery Plan
	6. Maritime Transportation System Security Plan
	7. Maritime Commerce Security Plan
	8. Domestic Outreach Plan

Table 1: National Strategy for Maritime Security (NSMS) strategies and supporting plans

The NSMS recognizes the commercial sector as an integral stakeholder, and mandates a cooperative effort between government and the private sector. The MIST process was born of a need to include the private sector early in the process of policy and technology development.

From the outset, the MIST team recognized the importance of coordinating with other national MDA efforts. Working closely with the MARAD, and joined later by OGMSA and GMAII, MIST focused their attentions at the local, practitioner level, to improve the effectiveness of new technologies and processes.⁴ At the same time that MIST focused on local needs, our national partners held the inaugural Global Maritime Information Sharing Symposium (GMISS) with a goal “to remove inhibitors to efficient commerce through enhanced information sharing.”⁵ To ensure that our local work efforts aligned with the national efforts, both organizations looked at incentives and models for information sharing and ways to streamline government requests. In addition, the MIST team probed for operational level goals, gaps, barriers and risks in the sharing of threat information and probed local port personnel for feedback on specific policies and technologies.

Why the private sector?

In the vast maritime domain, the private sector is integral to our nation’s economy and security. In the U.S. alone, we conduct 95% of our commercial trade on the water—moving over 2,000,000,000

³ <http://www.iaem.com/committees/GovernmentAffairs/documents/PPD-1.pdf>

⁴ Ulmann (2006)

⁵ OGMSA (2008)

tons of freight a year and handling \$264 billion in annual commerce.⁶ Federal policy recognized the importance of this in 2004:

“maritime security policies are most effective when the strategic importance of international trade, economic cooperation, and the free flow of commerce are considered appropriately.”⁷

Since a functionally robust economy is essential for our national well being, inclusion of the private sector is critical in any maritime security effort.

What are our challenges?

When talking about ways in which we can incorporate private sector input into the sharing of threat information and looking at the results of our workshops, two questions come to the forefront. First, given the massive network of agencies, applications, and programs⁸ involved in maritime security, how can we maximize collaboration between federal agencies and between federal agencies and the private sector? Second, given the central role of the federal government, how can we utilize network-centric theory to help us bridge existing communities?

Maximizing collaboration

As we’ve seen, federal stakeholders have embraced information sharing with the private sector, resulting in a large number of independent efforts. In fact, the GMISS 2008 report found that in the twelve months prior to their event, there were over 20 commercial outreach meetings scheduled by separate federal government entities. Unfortunately, these efforts may be disruptive to the movement of cargo and aggravate port efficiency⁹ as well as “over-whelming the intended dialog and actions.”¹⁰

In a 2002 report, the Government Accountability Office (GAO) noted this, finding that the building of critical partnerships is key to the national homeland security strategy:

“The complexity and urgency of the nation’s homeland security goals require effective, cooperative, and sustained action from multiple public and private entities, and addressing coordination and collaboration concerns will be vital to success.”¹¹

The National Strategy for Maritime Security goes further, contending that integrating all-source intelligence is essential for successful MDA, and that this effort will require “unprecedented cooperation among the various elements of the public and private sectors.”¹²

The challenge of maximizing collaboration is both economic and cultural. Even though many interagency coalition stakeholders generally agree that an MDA function is probably their responsibility, they are not able to spend funds outside of their respective departments.¹³ This lack of funding exacerbates the stovepipe or silo culture. In addition, the cultural constraints of

⁶ Renuart (2008)

⁷ The White House (2004)

⁸ OGMSA (2008)

⁹ Price (2004)

¹⁰ OGMSA (2008)

¹¹ GAO (2002)

¹² The White House (2005)

¹³ Walsh (2009)

organizations cause critical shortfalls in MDA which are “amplified by inadequate understanding of interagency capabilities and limitations.”¹⁴ These cultural constraints¹⁵ include:

- diverse missions
- conflicting goals and incentives
- engrained distrust
- non-collaborative leadership
- lack of coordination systems and structures needed to support collaborative efforts

Building systems that support collaboration requires a broad set of cultural shifts, including the alignment of incentives and the development of social capital. A recent report sponsored by NPS suggests that

“Although some individuals and organizations might collaborate because it is “the right thing to do,” collaborative capacity is reinforced by incentive systems that support doing ‘the right thing’.”¹⁶

In addition to incentives, effective collaboration between government agencies and the private sector requires that we address a broad range of social capital issues to consciously build collaborative capacity. Some of the social capital issues that can help build collaborative capacity include interpersonal trust, quality exchanges, and increased human interaction.¹⁷

There are many examples of how one might increase collaboration. A 2009 article on the Puget Sound Joint Harbor Operations Center (JHOC) highlights its key role in building collaborative capacity by “bringing all port stakeholders together with a shared goal – port and national security through information sharing and coordinated processes.”¹⁸ The report also notes how JHOC can further develop its collaborative capacity by increasing cooperative training and regular interoperability exercises.¹⁹ Our own research has shown how one Puget Sound group, the USCG Area Maritime Security Council (AMSC) program, has had some success at building collaborative capacity by coordinating planning, information sharing, and other necessary port security activities.

In the Puget Sound, the AMSC model of networked information sharing should be evaluated further as an example of local best practices in collaboration. The role of the federal government should be to facilitate this evaluation, share what they have learned with others, and ultimately, help to maximize collaboration.

Bridging Communities

The disconnect between the federal government and private sector maritime industry has been well documented²⁰. In response to this disconnect, the MIST process initially focused on building communities of interest around the sharing of threat information. We soon discovered that our message was not clear on the local level. The MIST process initially focused on building national communities of interest with established regional maritime communities around the sharing of security information. By adjusting our syntax to *bridging* these existing communities, we better

¹⁴ Walsh (2009) as noted by a 2008 North American Aerospace Defense Command (NORAD) and U.S. Northern Command (NORTHCOM) report

¹⁵ GAO (2002)

¹⁶ Fann Thomas (2006)

¹⁷ Fann Thomas (2006)

¹⁸ Metruck (2009)

¹⁹ Metruck (2009)

²⁰ OGMSA (2008)

communicate MIST's goal to improve the linkages between these often well-functioning groups, and reinforce our network-centric approach.

A net-centric approach, as used in this report, describes a loosely coupled information structure in which users deliver and receive information that enables operational capabilities across a range of missions. It presents a complete operating picture and is characterized by improved information sharing, improved situational awareness, increased collaboration, and improved responsiveness.²¹

Detective Candice Wright,²² currently serving as Port Security Coordinator in the Emergency Operations Division of the Long Beach Police Department, in her paper on applying network centric theory to the public/private sector shows how a network centric approach can create advantages specific to the sharing of maritime security information. Using the concepts embedded in network-centric warfare, she sees advantages in:

- Allowing autonomy in the execution of a commander's intent
- Supporting dispersed operations
- Eliminating procedural boundaries
- Improving timeliness, accuracy and relevance
- Speeding decision-making
- Adapting swiftly
- Focusing on achieving desired effects
- Helping to build shared awareness
- Expanding the use of networked sensors

A network-centric or federated approach results in a more flexible governance structure that can lead to faster response times and increased situational awareness. Within the private sector, there are many embedded network or federated models for communication: private sector shipping already has a high degree of situational awareness (through their global network of experienced mariners), they coordinate and synchronize with other companies and transportation providers, and their goal is speedy decision making and movement of goods and people.

The MIST process seeks to expand our concept of bridging communities through further examinations of existing network structures and information sharing systems. The federal role should be to identify these effective networks, then help bridge the gaps in the sharing of security information and cultivate the collaborative capacity of each port by partnering with local industry and maritime security players. MIST is in an ideal position to facilitate this network mapping.

In the next section, we present the findings from our research. These findings support the need for improved collaboration with the private sector and the use of a network-centric approach for information sharing.

²¹ Wright (2007)

²² Note: Detective Wright is a former student at the Naval Postgraduate School, now serving with the Long Beach Police Department, and a valuable member of the MIST advisory team.

Findings

In our prototype project in LA/LB, we focused primarily on identifying key issues in information sharing. For our Puget Sound event, we expanded our original focus to include a stronger focus on problem solving. To support these dual goals, we began, as before, by having our participants examine local issues related to incentives, information sharing practices, and areas for streamlining government activities. For this round, we also added specific activities designed to uncover local best practices, ideal information sharing criteria, and initial assessments of three information sharing programs (see sidebars on the AMSC p. 19, HOMEPORTR p. 21, and Dial “S-E-A” p. 17 programs).

Participants identified several areas that impact the effectiveness of sharing information with the private sector.

- Incentives and perceived benefits
- Performance measures that impact business operations
- Streamlining government requests
- Information flow

Incentives and perceived benefits

Incentives are key factors in the adoption of new process and policies. To align with our sister program GMISS, we focused in depth on what motivates the private sector to share information. As in LA/LB, we encouraged participants to look at the benefits of information sharing from a wide perspective. To help expand the concept of benefits, we presented participants with a 360 degree value model (see Figure 3) that segments value into five areas—financial, operational, social, ideological, and strategic. We encouraged participants to look at these benefits as they impacted them personally, organizationally and globally.

As in LA/LB, the participants identified operational efficiencies and the resulting financial benefits as the most important benefits of information sharing. In addition, they identified several social, ideological, and strategic benefits to information sharing that can help build buy-in, relationships and trust.

Following is a detailed discussion of the specific benefits that were identified by the workshop participants.

Financial benefits

“First you have to show me that there really is a threat out there— that’s why we’re spending all this money on it.”

When presented with the list of financial benefits from LA/LB the Puget Sound participants agreed that the following benefits were important:

- lower costs to vessels, operators, and customers
- personal rewards (recognition, financial incentives)

In addition, this port exposed new financial benefits related to the efficient use of resources and the design of processes tailored to local need:

- addressing the lack of resources related to the economic downturn
- sharing resources and capabilities to maximize impacts



Figure 3: 360° of Value
Value Segments and System Impacts

Findings

- reducing the impact on taxes from multiple “lessons learned” efforts
- avoiding “punitive fines for errors in reporting”
- addressing the impact of grant money lagging behind policy and requiring matching funds
- providing tailored information so that threat response is more efficient

Operational Benefits

“Efficiency (economic and social) is maximized through transparency and information sharing”

Operational benefits, which typically result in cost savings and higher revenues, were also key benefits for the Puget Sound group. Operational efficiencies that were shared with LA/LB included:

- Effective business resumption plans
- Efficient supply chain operations
- Consistent and predictable requirements
- Quick vessel turnaround
- Improved logistics
- Protection of assets

In addition, Puget Sound participants discussed issues related to the impact of the current economic downturn and the benefits of regulatory relief

- Reduction in resources is leading to doing minimal security efforts
- Sharing of resources helps reduce costs
- Fewer regulatory barriers leads to lower costs
- Local adaptations to the “intent” of rules helps reduce costs
- “Just-in-time” supply chain practices magnify the impacts of interruptions

Strategic benefits

“Like any multicultural group, when you get any group of employers together, they are going to find a common goal and work hard toward it, but will (also) focus on ‘what serves my needs’.”

A key goal for port operators is to encourage shipping companies to use the port. For individual companies it is protecting their assets and increasing their corporate advantage:

- Protecting ships and contents
- Improving ship security
- Making good business decisions
- Building good relationships, trust
- Improving customer service and public perception
- Environmental stewardship

Puget Sound participants also talked about how processes and collaboration affect strategy:

- Phased implementations can help with predictability
- Aligning with other groups can help strengthen the voice of smaller ports (American Association of Port Authorities for example)
- Aligning with and supporting port commissioners is necessary
- Jointly administering grants, exercises and drills improves strategic advantage for all
- Communicate value to upper management

Finally, the increased port use called for in LA/LB, was seen in the Puget Sound as being in conflict with increased public opposition to “traffic, noise, lights, and ugly container ships.”

Social benefits

“Because everyone has worked together for so long, there is a trust amongst us. This (trust) foundation facilitates info sharing”

As in LA/LB, participants identified a range of social benefits that could be used to incentivize information sharing. Specifically, they identified the following social benefits:

- Improved workplace atmosphere
- Feelings of inclusion for all port partners and government agencies
- Credibility and professionalism
- Pride of work
- Workplace rewards such as time off, promotions, and personal recognition
- Environmental stewardship

In addition, this port discussed the importance of trusted agents and good labor relations:

- Sharing technology, staff, capabilities, and best practices increases trusted agents
- A sense of interconnectedness leads to shared risk awareness
- Labor relations are an important factor, and should be addressed directly
- New security people struggle with getting established in the community
- A military approach can be off-putting

Ideological benefits

“Safety measures demonstrate the social value in protecting employees, citizens, and passengers”

Participants identified several ethical and political principles relevant to getting buy-in for information sharing:

- Improved safety
- Increased public trust
- Increased trust of government

Puget Sound, unlike LA/LB participants did not talk about the benefits of attaining *best of class* port status.

Recommendations

1. Modify requirements and processes to 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
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 communication with safety concerns

Findings

Performance measures that impact the business operation

“We need to maximize resources with minimal detractors”

When evaluating return on investment, the private sector has identified several performance measures that they feel are important:

Participants from LA/LB identified seven performance measures:

1. Time to access contact person
2. Total response time
3. Less time at anchor
4. Fewer delays
5. Fewer ships at anchor
6. Reduced violations (due to better information)
7. Sharp rate of decline in violations (when new policies are implemented)

Puget Sound participants expanded LA/LB measures to include three additional business metrics:

8. Decline in ground user complaints
9. More successful drills
10. More robust preparedness levels

Recommendations

10. Utilize an effects-based²³ approach to maritime strategy that includes private sector input

Streamlining government

Participants identified two key areas where government processes could be streamlined—interagency collaboration and minimizing the stove-pipe culture.

Increase interagency collaboration

“The further away you get from the flag pole of Washington DC, the smoother the flow”

In the Puget Sound, although there were challenges with dealing with federal agencies in general, participants were mostly happy with the interagency collaboration of their two main federal partners—the USCG and CBP. This was attributed mainly to local efforts. Key attributes of this successful collaboration were:

- Less stove piping at the local level
- Multiple areas of coordination (facilities security, infrastructure security, vessel security, information technology, law enforcement)

²³ An effects-based approach determines actions and policies based on the desired outcomes of stakeholders

Case Study: Dial “S-E-A”

Based on our findings in LA/LB, the MIST team selected a proposed GMISS policy implementation for concept testing. The concept was an “at sea” universal dial string (similar to 911) that could be used to report and retrieve MDA information. In evaluating the viability of the concept, participants looked at desirability, requirements, and implementation issues:

Desirability

Participants saw value in having “one number, one guy”, and “smart analysis and information flow” that allowed “access to needed resources.” However, on closer examination, the concept was not aligned with the internal processes of shipping companies—ships would use agents and superintendents instead, tugs would contact dispatchers directly, and port facilities would use internal communication processes first. In addition, there are legal and policy regulations that drive the private sectors communication flow.

Implementation challenges

Participants identified several key challenges in designing a one-stop system:

- Sustainability (funds and manning)
- Reliability
- Routing of calls
- Use of existing infrastructure
- Phased implementation
- Personnel/customer service
- Non-transmitting vessels
- Intermodal integration

Requirements

- Access to a wide amount of info
- Proprietary information protected
- Strong Navy coordination
- 24x7 access
- Excellent customer service (no lost calls, holds, transfers)
- Coordinated with current commercial reporting requirements

Findings

- Coordination of boarding and environmental threat mitigation efforts
- Strong Navy coordination
- Intermodal point of view
- Status as Pacific Northwest Economics Region
- Sense of interconnectedness and community
- Coordinated exercises
- Strong AMSC and FSO subcommittee

There were however, several areas where collaboration could be improved that were similar to LA/LB:

- Government agencies need to share among themselves better
- Government agencies need to provide one place for information
- Government agencies should have the role of reporting incidents to others
- Government agencies should sequence and compile all requirements

In addition, the participants identified several local hotspots:

- Stove piping at the federal level impedes communication (e.g. law enforcement access to SIPRNET)
- Multiple federal access points makes communication difficult
- FBI does not participate in regional exercises, resulting in poor collaboration between JTTF and ISAC.

Remove stove-pipes

“Choose a system and improve it, rather than improving all ten.”

In LA/LB, the participants discussed several policy conflicts that were not evident in the Puget Sound. In the Puget Sound, the key areas of regulatory challenges, included:

- Cross agency differences in IT policies (access to secure information, log-in policies)
- Complex programs
- Contact procedures differ
- Regulations not aligning with business requirements (e.g. perimeter barrier requirements impeded the flow of business operations)
- Unfunded mandates

Recommendations

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

Findings

Information flow

Good information flow is dependent on effective communication, easy access to information and quality information.

Improve communication

“When we’re on the dock if I don’t know anything about it, it doesn’t do any good”

Besides overcoming obstacles with government bureaucracy, the participants outlined several areas where communication with the government could be improved. As in LA/LB, the Puget Sound participants first and foremost identified the lack of sharing of threat information. In addition, they wanted to have a single point of contact for communicating issues and reporting threats and to have that communication include personal interactions with regulatory agencies. The Puget Sound participants noted the following needs related to communicating with MDA partners:

- Utilize waterfront residents as “your eyes and ears”
- “Go to the ground” with gathering threat information
- Align processes with regulations to “avoid punitive fines”
- Utilize the “feds to identify who and how states are sharing”
- Provide a system that “brings stakeholders together, validates concerns, gives direction and procedures”
- Provide a central contact for notifications and information distribution
- Government agencies “should have the role of reporting incidents to others”
- Provide good customer service and don’t “put the caller on hold”, or “transfer them and get lost” or not return calls

In addition, for the Puget Sound workshop, we probed the relationships between the private sector, federal and international partners, local and state partners, and other commercial entities. We identified numerous agencies that require coordination around MDA issues:

Federal and international partners

- MSSIS – DOT Volpe Center²⁴
- Regional maritime ops centers²⁵
- U.S. State Department OSAC
- MARLO (Maritime Liaison Office)

²⁴ <http://www.volpe.dot.gov/>

²⁵ Such as PACCOC, Straits of Malacca regional group, NATO, AFRICOM’s nonclassified ops picture of Horn of Africa

Case Study: Seattle AMSC

The Seattle sector Area Maritime Security Council (AMSC) serves the ports of the Puget Sound. Its focus is on collaboration, and mission and policy planning.

Value

Seattle’s AMSC is highly valued and is seen as one of the local “best practices.” It is valued for:

- Building relationships and trust
- Focus on function
- Increased communication
- Shared standards and practices
- Joint operations

Evolution

The AMSC in Seattle has evolved over time to a “zenith” position. Recently, the appointment of a new Captain of the Port (COTP) has resulted in major changes to the AMSC, which impacts stakeholders. For instance, the creation of a new Executive Committee with topic focused subcommittees formalized practices and offered opportunities to be more “productive, interactive, and engaging.” Although some members initially felt removed from the process; subcommittee members perform the real work and have a voice on the issues. Changes in COTP’s, by nature, can be disruptive to the local community and participants suggested including local representatives in a continuing role in order to ease transitions in COTP’s. The AMSC Co-Chair position was created and is held by a local representative of the maritime community.

Notables

The Facility Security Subcommittee has been operating for a few years and is valued as a reliable regional resource for sharing information and facility security practices. In addition, the AMSC recently formed an Information Sharing Subcommittee, which participated in the MIST workshop as part of their start up activities.

Findings

State and Local Partners

- HazMat/local Fire
- NW Warn
- Port of Seattle Police
- Puget Sound area governments
- Seattle Fire Department
- Seattle Police Department
- Harbor Patrol
- Port of Tacoma Maritime Information Support Team
- Transportation Sector Coordinating Council (TSCC)
- USCG FIST
- Washington DOT
- Washington Emergency Management
- Washington Ferries
- Washington Fusion Center
- Washington Infrastructure Protection Subcommittee (IPSC)
- Washington State Patrol

Commercial Partners

- AAPA
- CAPA (NorCal)
- Bloomberg
- CAL Maritime
- ISAAC
- Lloyds of London
- Washington Public Port Association (WPPA)
- Marina Association (small boats)
- Marine Exchange
- Pacific Northwest Economic Region (PNWER)
- NW Marine Terminal Association
- Jones Stevedoring and SSA Marine

Participants broke into small groups and identified several best practices for improving communication:

- Use a variety of communication tools—face-to-face, web, emails, newsletters
- Encourage wide participation—maritime roles, small and large ports, all functions
- Support networking
- Build trust
- Strengthen the functional focus
- Leverage local resources
- Keep direct contact with work force

Streamline access to information

“We need to have some synergy...if you have everyone calling in, what is the infrastructure to direct the information?”

A key barrier to information sharing is getting access to the information. Puget Sound participants, like their LA/LB counterparts, need a central repository for information and requirements, need access to be easy, and need to be able to have some access to classified information. Specifically, participants identified a need for:

- Pushing out information to the people who need it
- Gaining access to needed intelligence information (e.g. threat information)
- Having access to relevant classified information
- Providing a one-stop place for incident reporting
- Providing a one-stop place for all maritime requirements
- Standardizing data collection methods

Findings

- Linking between resources (e.g. HOMEPORT and MarView)
- Opening up closed systems (e.g. law enforcement)

We also probed participants for characteristics of an “ideal” information delivery system:

- Info pushed out to you, don’t have to go digging
- Info/event tagged then put in a bucket – can check back for updates
- Anytime, anywhere alerts in real time (e.g.. Alaska Airlines on flight changes, new info)
- Customizable to your personal interests

Improve the quality of information and tools

“Give us something to work with. Is it homegrown eco-terrorists or international level cells I need to worry about?”

Participants identified a need for information that is relevant and is designed at the appropriate level of detail. Specifically, participants noted several issues that reduced the effectiveness of the information system:

- Information is not pertinent to their local needs and work outcomes (protect ships, keep the port safe, track ships locally and globally)
- Inadequate structures to facilitate trend analysis
- Data is not synchronized with other processes
- Systems and data are duplicated

Participants were also asked to identify key functional requirements for an “ideal” information system:

Data qualities

- Provide live, real-time, self-correcting data
- Provide actionable data that is specific to the individual
- Make sanitized data available
- Perform trend analysis (regional, state, federal, global)
- Synchronize processes, data requests, data summaries (Washington Emergency Management may be a good model)
- Communicate project outcomes
- Clarify reasons behind specific actions
- Present an intermodal point of view

Information types

- Regionally targeted information
- All hazards
- Situational awareness
- Impacts on cargo flows
- Functional impacts (e.g.. biological threat)
- Neighborhood alerts
- Resource library (who’s who, where, counterparts in other ports)

Case Study: HOMEPORT

Because LA/LB and Puget Sound participants identified HOMEPORT as a key information sharing source, we had participants look at the desirability, usefulness, and ease of use of the system.

Desirable

A collaborative web tool developed and maintained by the USCG, HOMEPORT is one of the top tools mentioned by port security personnel; although participants noted that it appears to be targeted primarily at USCG personnel. Users see two values to HOMEPORT—as a collaboration tool and as an information source. Participants would like to see HOMEPORT tailored to common topics that affect their everyday working lives, for example, security and pollution issues.

Useful

When doing an *information seeking* task, participants found that HOMEPORT was not very useful. The local site was designed as a collaboration tool and therefore was not serving an information sharing function. Because HOMEPORT relies on local resources to develop content, its usefulness is limited by resource constraints and local prioritization of function. This distinction is not clear on the site and users are confused about whom it serves.

Easy to Use

Functionally, HOMEPORT has several usability problems which limit its effectiveness:

- Password policies deter users
- Key material is available only in password protected areas
- Value-rich SSI information is only available to authorized users
- Drilling down through geographic criteria is confusing
- Users want topic driven menus (e.g. security, safety, etc.)
- Menu options are not in “plain and simple language”

Usability

- User profiles based on “community of interests”
- Single government voice
- Trustworthy, accurate information source (that isn’t scooped by media)
- Simple language, clearly summarized (not just pie charts)
- Executive summary upfront, supporting evidence behind

Recommendations

16. Give a single agency the power and resources to support quality communication:
 - *Support local networking, include direct contact with workforce*
 - *Leverage local resources*
 - *Have diverse roles, ports, and functions*
 - *Connect regional partners with state and federal agencies*
 - *Coordinate federal MDA activities, resources, and data*
 - *Manage a central reporting system*
 - *Integrate the central reporting system with a central sharing system*
 - *Align MDA processes with regulations*
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)



Lessons Learned

The way forward

Private sector input is integral to the design of any maritime threat information sharing process. Through the MIST process, we hope to move toward presenting an appropriately weighted message from those who will be impacted most directly. Building on our first two successful efforts, MIST will continue to identify “best practices” and “hotspots” in individual port communities that will inform successful MDA efforts on the federal and global level.

Recommendations

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

Lessons learned about MIST processes

In this, our second full round of MIST, we further refined our process and came away with some actionable design modifications.

Outreach

To aid with workshop planning and recruiting, our collaborative outreach effort included representatives from many federal and local organizations²⁶ in the MIST Puget Sound Steering Committee. To maximize steering committee member participation, we will investigate how to make it easier for those at the federal level to participate. Recognizing that MARAD had competing priorities on the federal level in light of recent international piracy events, allowed us to shift our expectations of their federal and local representative engagement. We also noted a need to garner more visible participation by major stakeholders such as USCG and CBP.

The process could also be improved by increasing the participation of additional stakeholder groups such as labor unions, local academia, local law enforcement fusion centers and private sector representatives. These additional stakeholders should also be more engaged in the final workshop.

We have learned that the concept of the MIST process is most effectively presented in face-to-face briefings. Outreach at future MIST port sites will include presentations to the local AMSC Executive Committee or General Membership meetings in the months prior to the scheduled workshop. We will also actively pursue additional local presentation opportunities to bolster understanding of the MIST mission, and to aid participant recruitment efforts of our local steering committee members. For the MIST Puget Sound effort, the steering committee generated a potential invitee list from individual contact lists, and knowledge of the local port working environment. Although the quality of information on this list was exceptional, for future efforts we will also generate a 'cold' list in advance of the first steering committee meeting to augment recruitment. Sources to mine for

²⁶ Marine Exchange of Puget Sound, the Port of Seattle, the USCG Sector Seattle, Seattle NCAGS, Port of Seattle CBP, and MARAD Seattle OGMSA, GMAIL, USCG, MARAD, NCAGS and NPS

potential participants include: DOT-MARAD, the local Marine Exchange, the local Port Authority, the AMSC, as well as the Internet.

To facilitate tracking of participation status, we will assign one person to manage the invitee list. This allows for weekly recruiting progress reports and required participant contact to foster relationship development between MIST team members and participants prior to the workshop. In establishing a relationship with the MIST process and team, we anticipate increased productivity from the final workshop event.

Website

In preparation for the MIST Puget Sound process, we worked closely with MARAD to design the MIST website.²⁷ Much of the design was informed by the MIST LA/LB findings, however local resources were added following the March 2009 MIST Puget Sound reception. While it was encouraging that the participants used the site (evidenced by links from other sites to MIST) the site was not used as envisioned. Specifically, the social networking tool was not used. Local workshop participants use existing tools (such as LinkedIn), and found the MIST Member page duplicated other efforts. However, through the iterative MIST website design process we were able to capture local user needs effectively. For example, an acronym list was added in response to a steering committee request. Although the MIST Help Desk²⁸ received few calls, we learned that any participant/member request (phone, email, face-to-face) needs to be logged for use in future reporting. Lastly, posting a link to the MIST website on the local link for HOMEPORT and MarView could be a potentially high return outreach action.

Preliminary events and activities

The MIST Puget Sound process expanded on the core MIST LA/LB Workshop event in two key ways. First, a field study component was added involving site visits and interviews of a range of private sector maritime industry work environments. Second, a face-to-face MIST Puget Sound Reception event was held in March 2009 at the National Oceanographic and Atmospheric Administration (NOAA) campus just north of downtown Seattle. With the guidance of local steering committee members, field study participants were selected, contacted, and scheduled. The Human Subjects application process through NPS was completed with ease. However, if the field study component is included in future MIST processes, alterations informed by the MIST Puget Sound experience may include: additional preparation for interviews (to help standardize results with more than one interviewer working concurrently); schedule one interview per day rather than two (to allow time to review notes immediately, then prepare for the next visit); review transcription process including software capability and user training; evaluate potential participants' value as a workshop participant or interview subject.

The MIST Puget Sound reception held two months prior to the final workshop event was a productive addition to the process. Meeting steering committee members and potential participants ahead of the workshop fostered a more collaborative environment for the rest of the process. The reception also allowed for a face-to-face briefing of the MIST process, established as the most effective mode to convey this unique concept. The site visits for potential reception venues incorporated into a conference trip for DHS Science and Technology Directorate in February 2009 allowed the MIST team to make the best choice for the reception. Combining the field study with the reception proved to be an effective use of MIST facilitation team travel time and resources

²⁷ www.marview.gov/mist

²⁸ (831) 656-2198

Structure and design

Upon review, workshop structure and design modifications were identified to maximize workshop outcomes. Structurally, it is felt that including more demonstrations of local information sharing models would breakup sections of the workshop that were primarily theory related, and might spur creativity in the group breakout sessions. An important design alteration for the next MIST process is first to generate information from group, then display the model. Some participants felt “boxed in” when presented with a visible theoretical outline slide, and feedback potential may have been affected. Additionally, the presentation of the LA/LB workshop results in concert with the presentation of topic may have implied boundaries, or subconscious suggestive responses could have altered feedback, skewing final results and findings.

RDML Roy Nash, USCG 13th District Chief of Staff, proved to be great choice for the keynote introductory remarks. His presentation slides were clean and effective, and the sharing of For Official Use Only (FOUO) classified information set a nice example of collaborative security information sharing – displaying trust in local private sector stakeholders, and fostering goodwill and growing social capital.

Small group break-outs several times during the workshop helped ensure that the MIST process captured all participant voices. It also helped us stick to the prescribed format. Live capture note taking yielded a rich data source for coding, without the ramifications of a recording device. However, it was suggested that the MIST facilitators review the daily notes to help improve the flow of the workshop in to the second day, highlighting accomplishments and direction.

Both facilitator and participant feedback indicated that the day and a half time frame was just about right for the subject areas covered. Requests included more time at the end of the workshop for feedback and critique, and more time spent on demonstrations of local information sharing models in the Tools section of the workshop.

Logistics

The second floor conference room of the Port of Seattle headquarters building is a great room in a very nice facility. While the standard meeting supplies were ample, internet access essential for the MIST process, was challenging. Future MIST processes will need to arrange for concurrent internet conductivity on multiple laptops to maximize the effectiveness of breakout sessions. Although the small breakout groups worked well in the space available, one group had trouble hearing each other. For next round, an acoustic check of potential breakout locations would benefit the process.

Coffee and pastries provided by the Marine Exchange of Puget Sound on the morning of the first day set a congenial tone for the work ahead. When food is provided, it generally improves the mood of the group. Unfortunately, the capacity of government agencies to provide food for any event is constrained. The stakeholders group should address this challenge early on in the planning so that it is not a last minute logistical item.

The NPS MIST planning team engaged in a 'hot wash' that surfaced the above lessons learned the week after the workshop. In the future, it may be useful to engage the steering committee in a hotwash process to validate findings immediately after the workshop in addition to their engagement of report reviewing prior to final release.

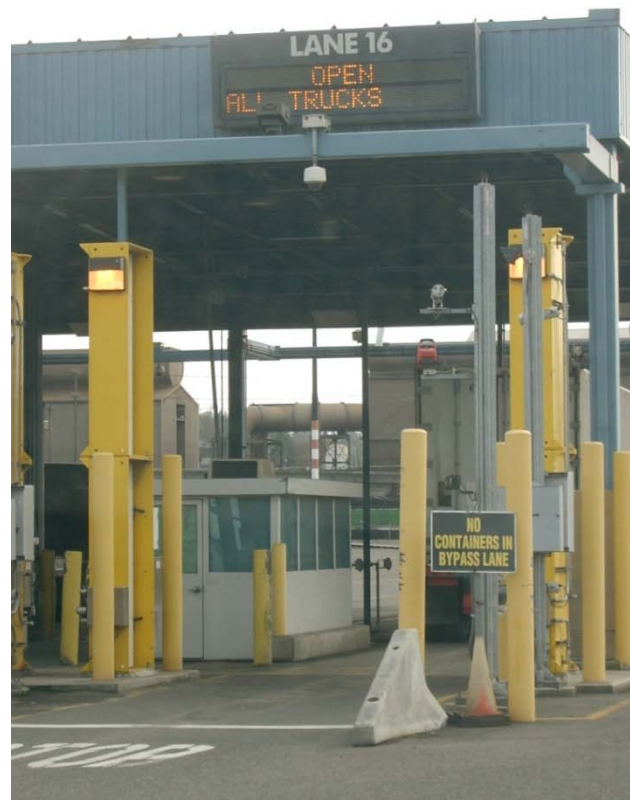
Recommendations

26. Add stakeholder representation from:

- *labor unions*
- *local academia*
- *local law enforcement fusion centers*
- *and increase private sector representation*

Lessons Learned

27. Outreach presentations to the local AMSC Executive Committee or General Membership meetings in the months prior to the MIST event
28. To facilitate tracking of participation status, we will assign one person to manage the invitee list.
29. For the field study:
 - *additional preparation for interviews to help standardize results with more than one interviewer working concurrently*
 - *schedule one interview per day rather than two to allow time to review notes immediately, then prepare for the next visit*
 - *review transcription process including software capability and user training; evaluate potential participants' value as a workshop participant or interview subject*
30. Review the daily notes to improve the flow of the workshop in to the second day, highlighting accomplishments and direction
31. Add more time at the end of the workshop for feedback and critique
32. More time allocated to demonstrations of local information sharing models.
33. Arrange for concurrent internet conductivity on multiple laptops to maximize the effectiveness of breakout sessions
34. Address refreshment logistics early
35. Engage the steering committee in a hotwash process to validate findings immediately after the workshop



Appendix A: Methods

For the second round of MIST, we again targeted port stakeholders involved with MDA, but this time focusing on the Puget Sound region. In this section, we review the purpose and scope of the process as it relates to the targeted stakeholders; focused participant recruiting efforts; preliminary activities in the region in support of the MIST process; the interactive website tool; and conclude with a more detailed discussion of the workshop design itself.

Using an iterative participatory approach, the researchers partnered with federal, local and private sector stakeholders to assess the information sharing needs of security personnel in the maritime port communities of the Puget Sound region. The resulting research design included an issues workshop, field studies of port personnel, a local networking event, and a wiki-model process website.

Stakeholders

Purpose

The mission statement of MIST is: *To create a process for international, bi-lateral sharing of maritime threat information between private sector shipping and government agencies. This process must mitigate the concerns of private industry and provide value to both parties.*

Scope

Because of the complexity of the maritime domain and the lack of similar programs, the initial effort was viewed as a phased process. The first phase included the formation of a working group that was tasked with identifying key strategic, operational, financial, ideological, and social values and resistances –MIST. Due to time and budget constraints, we decided to pilot the process at the combined Ports of Long Beach and Los Angeles and targeted a cross section of the private and public sector. Based on the results of the pilot workshop, we modified our process prior to our next regional workshop in the Puget Sound region.

Participant recruiting

For the second in our series of workshops, we targeted commercial and facilities security officers. These key stakeholders were identified in our initial workshop as those who have the most access to threat information, the most impacted by regulatory issues, and those that make information sharing decisions in real time. As in our preparation for the LA/LB round, we established an advisory team to assist us in refining the mission and helping to recruit participants. This MIST Puget Sound steering committee included representatives from NPS, MARAD (federal and local), USCG (federal and local), local CBP, local Port Authorities, the Pacific Northwest NOAA, and the Marine Exchange. The MIST Puget Sound Steering Committee was tasked with contacting and getting commitments from key local stakeholders. As in LA/LB, we wanted to include federal level participation and invited representatives from the USCG and CBP, NORTHCOM, OGMSA, GMAII and DOT-MARAD. Final attendees included representatives from the following agencies and port stakeholders: CBP, container terminal security, DOT (MARAD and Washington State Ferries), GMAII, OGMSA/GMISS, labor/terminal workforce, the Marine Exchange of Puget Sound, Port of Everett, Port of Seattle, Port of Tacoma, shipping industry, tugboats, the JHOC, and both federal and local USCG.

Preliminary activities

Building on our progress, we altered the schedule of the entire MIST round somewhat, adding a preliminary face-to-face reception event two months prior to the workshop. We also combined a

field study element, conducting interviews and site visits at a variety of commercial enterprises in the region.

Website

To support community building and provide a place for information sharing, we designed a website for use prior to the workshop. The website was implemented but did not go live prior to the LA/LB workshop. The website was hosted on MarView, A DOT-MARAD website that *“provides the ability to fuse data together to create models and simulations for capacity planning, economic impact analysis, on-demand forecasting, plans for mitigating and reacting to emergency situations”*²⁹. The MIST website was designed for pre-conference information sharing, as a social networking tool, and a place for MIST members to review, edit, and add information relevant to their needs.

MIST Homepage

The MIST website included: useful resources, member polls, member profiles, a member forum, and an events calendar. Links to all sections appeared on the home page.

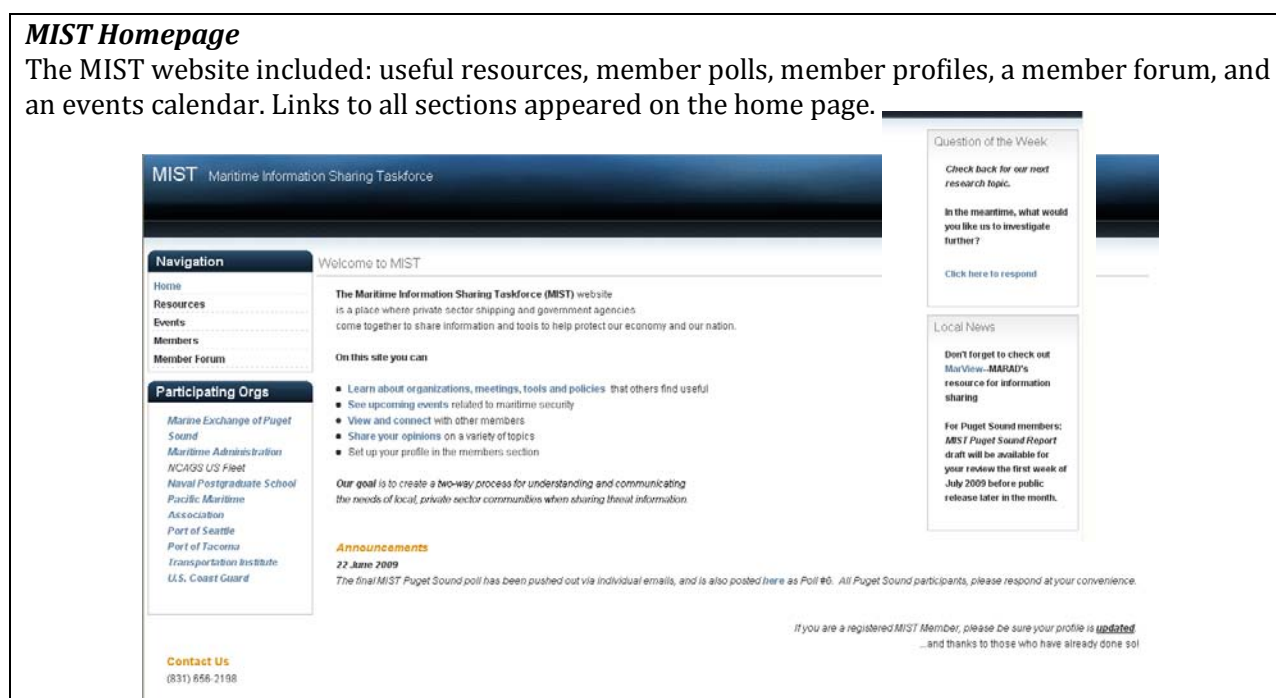


Figure 4: MIST Homepage

²⁹ www.marview.gov

Resources

The resource section includes local, state, and federal resources—organizations, meetings, and tools—that might be useful for sharing maritime threat information. Users could also add new, rate and comment on the resources.

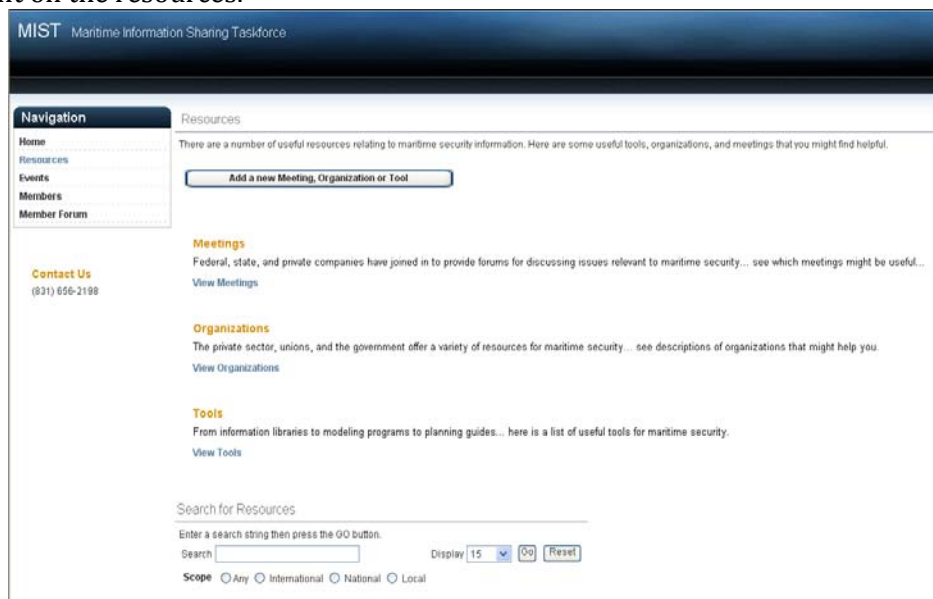


Figure 5: MIST Resources

Member Profiles

To help build a sense of community, we implemented a social network function that allows members to post biographies and contact information.

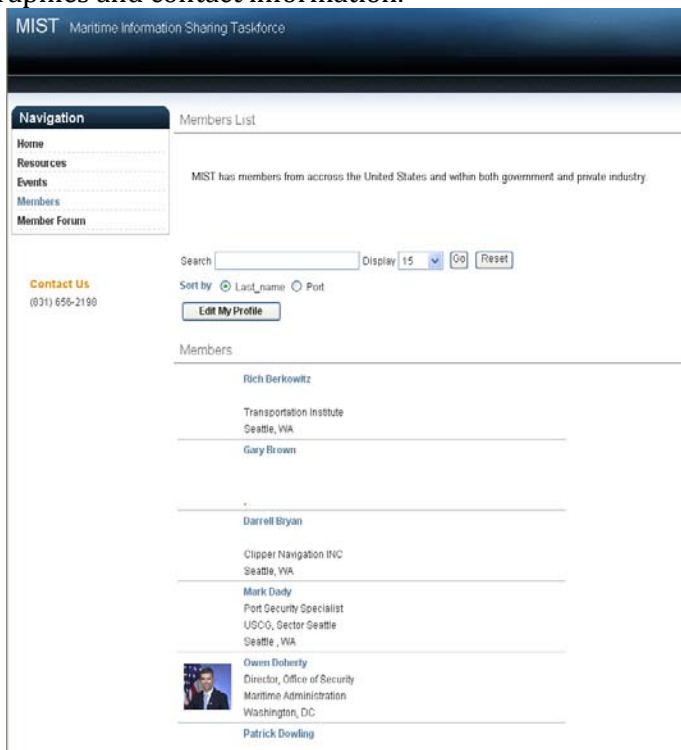
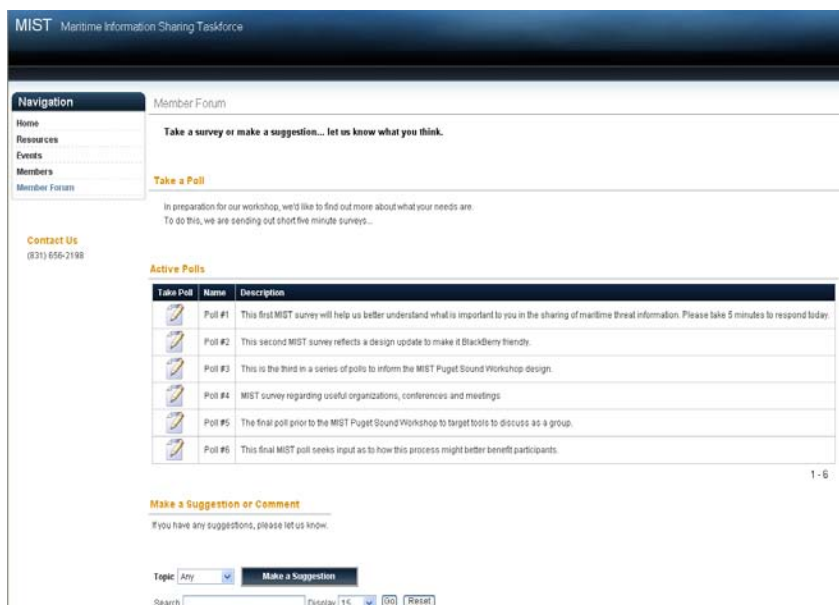


Figure 6: MIST Member Profiles

Member Forum

The member forum provides access to completed polls, new polls, and user comments.

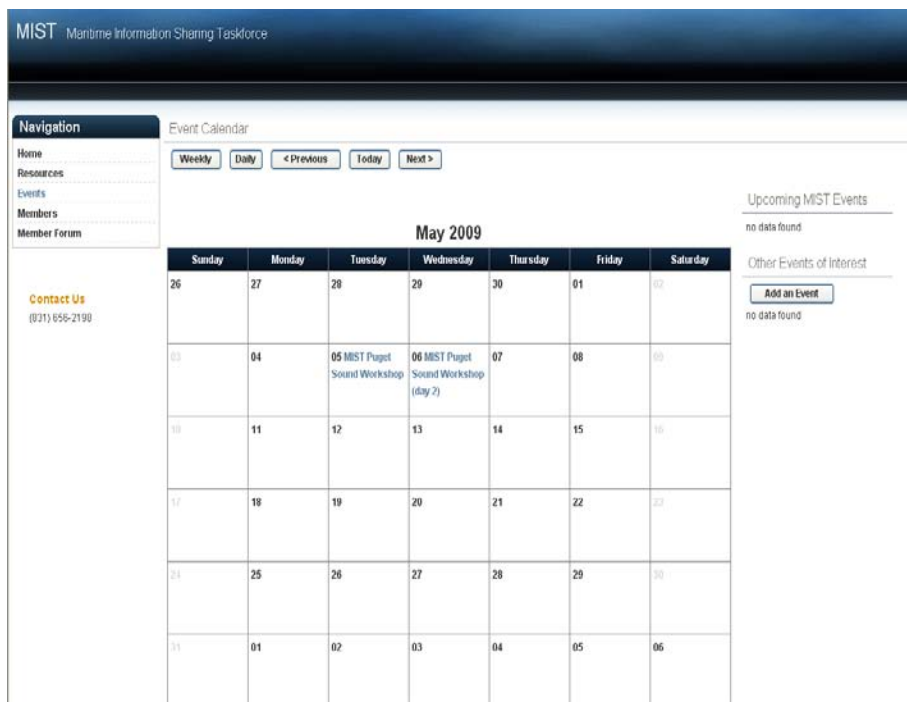


Take Poll	Name	Description
	Poll #1	This first MIST survey will help us better understand what is important to you in the sharing of maritime threat information. Please take 5 minutes to respond today.
	Poll #2	This second MIST survey reflects a design update to make it BlackBerry friendly.
	Poll #3	This is the third in a series of polls to inform the MIST Puget Sound Workshop design.
	Poll #4	MIST survey regarding useful organizations, conferences and meetings.
	Poll #5	The final poll prior to the MIST Puget Sound Workshop to target tools to discuss as a group.
	Poll #6	This final MIST poll seeks input as to how this process might better benefit participants.

Figure 7: MIST Member Forum

Events calendar

The calendar provides access to local and national events of interest.



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
26	27	28	29	30	01	02
03	04	05 MIST Puget Sound Workshop	06 MIST Puget Sound Workshop (day 2)	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	01	02	03	04	05	06

Figure 8: MIST Events calendar

Workshop

Although similar in design to the MIST LA/LB workshop, the focus in the Puget Sound moved to our second tier benchmarks – information flow and community bridging. The workshop itself was spread over two days. We designed the workshop to maximize interaction and allow for both individual and group identification of issues. There were two primary facilitators from NPS who led small and large group discussions. We also had three presenters who introduced the current MDA information-sharing network from the intelligence community's point of view, USCG's HOMEPORT web tool, and a proposed "one-stop-shop" for maritime threat information sharing – Dial "S-E-A."

Using PowerPoint as an organizing tool, we had participants do small group brainstorming and large group synthesis. In the slides, we provided clear instructions to the participants and provided visual clues on process for the facilitators. In the workshop, we explored six areas:

1. *Streamlining government requests:*
In this section, we had participants identify, discuss, and rank government requests that were difficult. The participants used one dollar stickers to mark those items that they felt were the most important.
2. *Incentives for information sharing:*
Using a 360 degree value model, we had participants identify, discuss, and rank specific benefits that could be used to incentivize the private industry.
3. *Tools for information sharing:*
Participants were guided through a discussion of current tools, analysed their usefulness, then were introduced to a current and proposed tool for testing and evaluation.
4. *Partner issues in information sharing:*
In this section, we asked participants to identify and evaluate relationships between partner organizations at the local, federal, and international level.
5. *Models for Information Sharing:*
This first new module on the second day of the workshop identified local best practice models, thoroughly evaluated those models, then allowed participants to brainstorm and define their collective ideal maritime threat information sharing model.
6. *Next Steps:*
The final activity for the workshop was to discuss how we could move forward and communicate better.





MIST Puget Sound Workshop, 5-6 May 2009 WORKSHOP AGENDA

Tuesday, 5 May

- 0800-0900 **Registration /Networking**
- 0900-0930 **About MIST-** overview of the project and desired outcome of this workshop
 Wendy Walsh, NPS and Anita Salem, NPS
- 0930-0950 **Key Note Address**
 RDML Roy Nash, USCG
- 0950-1000 **Break**
- 1000-1130 **Streamlining Government Requests**
 Patrick Dowling, USCG and Anita Salem, NPS
- 1130-1300 **Lunch**
- 1300-1400 **Incentives for Sharing**
 Anita Salem, NPS
- 1400-1415 **Tools for Information Sharing (1)**
 LCDR John Taylor, USCG and Anita Salem, NPS
- 1415 – 1430 **Break**
- 1430-1530 **Tools for Information Sharing (2)**
- 1530-1700 **Partner Organization Issues**
 Tim Phillips, GMAIL and Anita Salem, NPS
- 1700 **Day One Wrap**

Wednesday, May 6

- 0830-0900 **Check in / Networking**
- 0900-1030 **Models for Information Sharing – AMSC, JHOC, JTTF**
 Rod Hilden, Port of Seattle and Wendy Walsh, NPS
- 1045-1200 **Next Steps – Solution Exploration Review**
 Final Discussion: facilitated by Anita Salem and Wendy Walsh, NPS
- 1200 **Adjourn**

Appendix B: Survey and Evaluation Results

Pre-workshop surveys

Methodology

To prepare for the MIST Puget Sound Reception in March 2009, followed by the MIST Puget Sound Workshop in May 2009, we sent out five polls by email to all identified potential participants. We designed these polls to be brief and quickly answered. In response to a suggestion, beginning with the second poll, they are designed to be BlackBerry accessible.

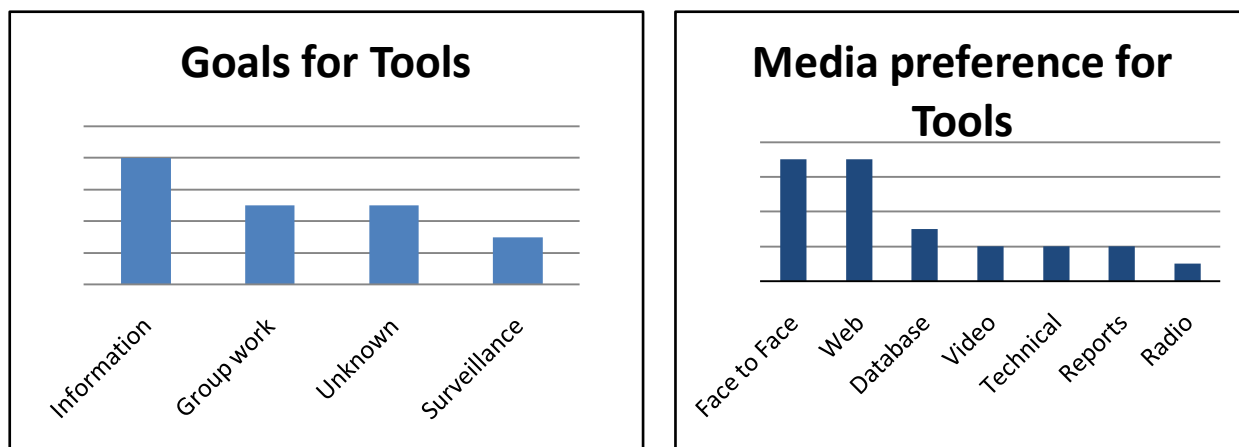


Figure 9: MIST pre-workshop survey results

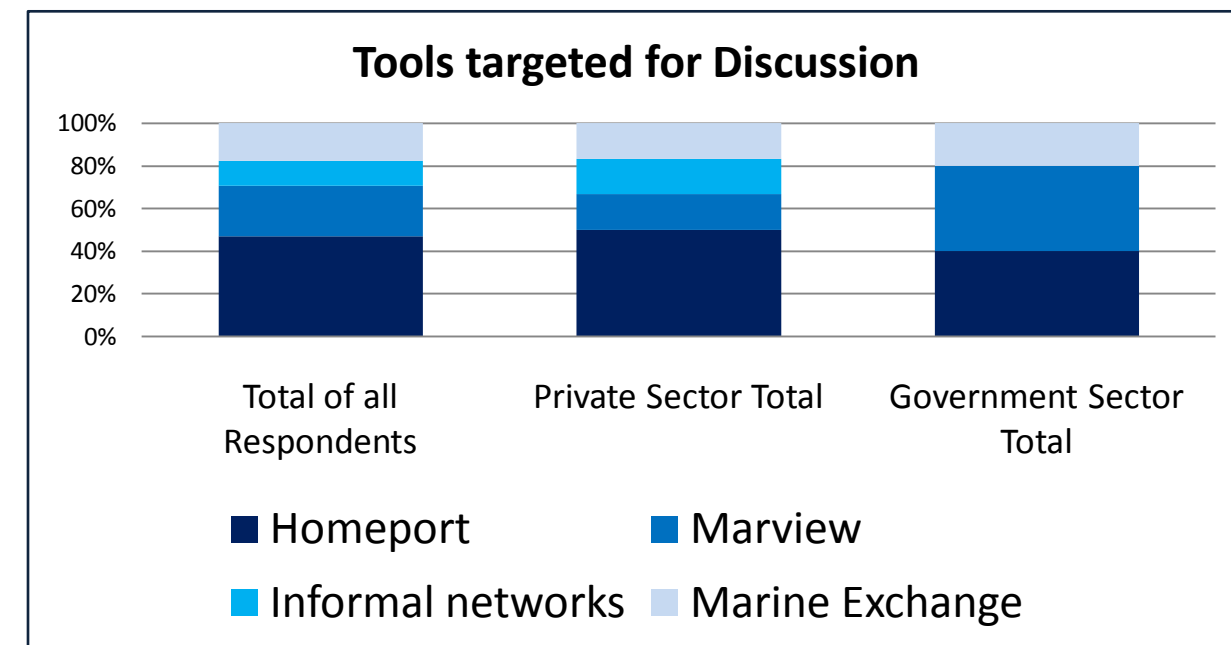


Figure 10: MIST pre-workshop survey results (2)

Workshop evaluation results

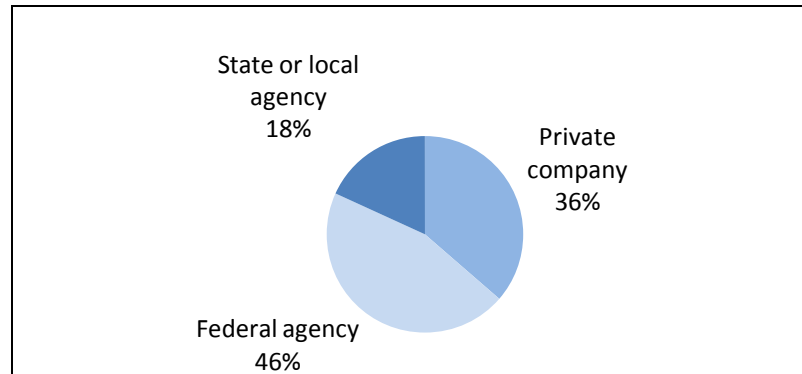


Figure 11: MIST Puget Sound Workshop participant affiliations

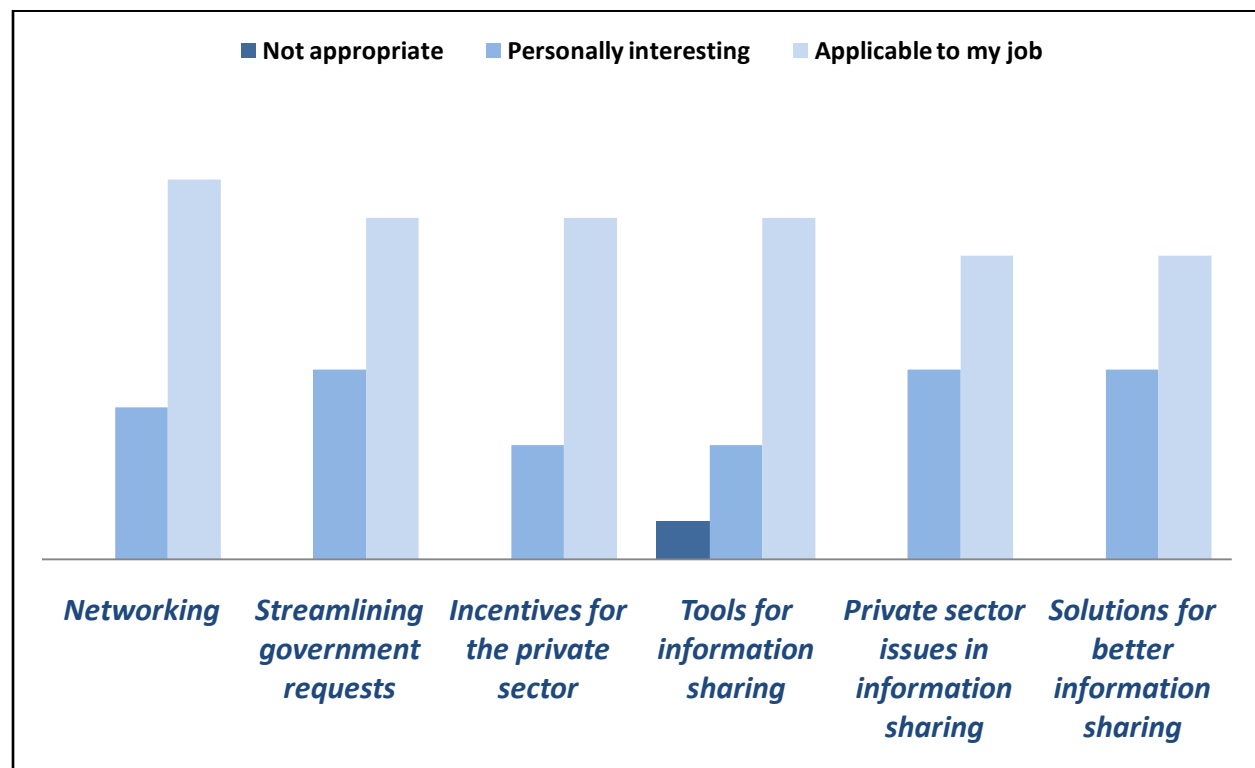


Figure 12: "How appropriate were the topics discussed?"

<u>QUESTION</u>	<u>AVERAGE RESPONSE</u> <i>on a 4 point scale except where noted</i>
Overall, how well organized was this workshop?	4
Overall, how useful was this workshop?	3.5
How effective were the individual sessions in helping identify issues with sharing information?	
Presentations	2.7 of 3
Large groups	2.5 of 3
Small groups	2.2 of 3
How likely would you be to do the following?	
Read background information before the event:	3.4
Use the website before the workshop:	3.5
Use the website after the workshop:	3.4
Set up your personal profile on the web:	3.6
Add a resource to the website:	2.6
Recommend this workshop to others:	3.5
Continue to participate in information sharing activities:	3.8
The workshop was:	
Too long:	1.9
Too short:	2.1
Made me feel rushed:	2
Was too slow:	1.4
Did not provide enough breaks:	1.3

Table 2: MIST Puget Sound workshop evaluation average responses

Comments on format and effectiveness:

- Got off track too often
- Lost control on Friday morning
- Felt like there were predetermined results the group was looking for
- Once your audience is targeted, hound them to get a more diverse audience
- Some concern that not enough people from industry participated in small groups to provide representative data

Comment on time frame:

- Although seemingly long, this is a huge subject and more time could be spend on it – question being would it be any more productive if it were longer?

General comment:

- Well managed presentations and discussions

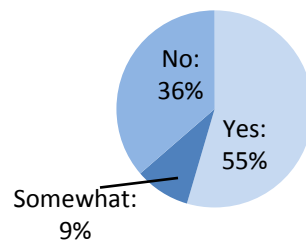


Figure 13: "Were the right people in attendance to capture the needs of the private sector?"

If no, who would you include?

- **Commercial:**
 - Not enough BCOs (*beneficial cargo owners*), lines, operators
 - No fishing industry.
 - Shipyard
 - Vessel captain
 - Agent
 - More commercial / FSOs
 - I would like to see more trade groups from marine industry (PMSA, WSPA, AWO)
- **State and Local:**
 - Local law enforcement
 - Local law enforcement
 - Needed local law enforcement and DOJ
 - State environmental
- **More participants needed overall**
 - I was disappointed that certain segments weren't represented
 - More additional maritime stakeholders
 - Too few overall.
 - Probably not diverse enough. A lot of perspective from one source

In future workshops, what would you have us do MORE of?

- Polling around the room to each participant rather than letting a few dominate
- Actual demonstration of MarView and other intelligence sharing websites
- I know time is of the essence, as well as covering all your bases, but perhaps find a way to let conversations overflow
- Presentations from local agencies
- Keep on track with subject and time – more focused/structured. More diversity in attendees.

In future workshops, what would you have us do LESS of?

- Less strict time frame for each segment. Be flexible, but keep timing to yourselves.
- Less small groups and pre-designated topics. Felt like the group focus was determined by outcomes of LA/LB group. That was a different group than in Seattle. LA/LB was more port people, while Seattle group was more facility, private sector, and government.
- Just right
- Everything was relevant

Follow up survey

Response

A total of seven participants responded to the follow up poll. When asked about proposed tangible benefits, the majority were interested in an official letter of participation from an appropriate federal level security official. There was also significant interest in a MIST findings summary document designed to be easily inserted in future Port Security Grant applications. Respondents expressed interest in a presentation including Port Security Grant application tips from a federal level review, and suggested inclusion in future workshop design.

Results were mixed when asked to identify the most important issue discussed at the workshop. Four of the seven respondents felt that coordination, communication and streamlining were the most important issues discussed. However, partner organizations, agencies and organizations, as well as best practices and ideal system design were also noted.



Appendix C: Survey and Evaluation Instruments

Pre-workshop

MIST Poll #1: This first survey will help us better understand what is important to you in the sharing of maritime threat information. Please take 5 minutes to respond today.

1. Your roll in maritime security is: (select one)
 - ☐ Facility Operations
 - ☐ Vessel Operations
 - ☐ Law Enforcement
 - ☐ Shipper
 - ☐ Other (specify below)

2. Your organization is a: (select one)
 - ☐ Private company
 - ☐ Public association
 - ☐ Federal agency
 - ☐ State or local agency
 - ☐ Other (specify below)

3. When it comes to maritime security, your organization needs more collaboration between the public and private sector.
 - ☐ Strongly Disagree
 - ☐ Disagree
 - ☐ Agree
 - ☐ Strongly Agree

4. In your daily work, what are your three most pressing problems with sharing information?

5. For you, the THREE MOST important issues to address in the sharing of threat information are: (mark only three)
 - ☐ Clarification on roles and responsibilities
 - ☐ Intelligence reports
 - ☐ Live situational awareness tools
 - ☐ Recovery and mitigation efforts
 - ☐ Reporting procedures and guidelines
 - ☐ Other (please specify below)

6. In your work in maritime security, the THREE AREAS that you are most concerned about are: (mark only three)
 - ☐ Access controls (people, barriers, guards and surveillance)
 - ☐ Cargo inspections
 - ☐ Cargo theft
 - ☐ Data management
 - ☐ International issues
 - ☐ Military and law enforcement response capabilities
 - ☐ Planning for disaster recovery and continuity of business
 - ☐ Shipping, trucking and rail connections
 - ☐ Vessel operations
 - ☐ Other (please specify below)

7. During the upcoming workshop on the sharing of maritime threat information, what one issue do you think we should try to analyze and solve?



MIST Poll #2: This second survey reflects a design update to make it BlackBerry friendly.

1. When talking about the sharing of threat information, what information do you want? Please be specific.
2. You are from the private sector:
 - ☐ Yes
 - ☐ No
 - ☐
3. Your role is:

MIST Poll #3: This is the third in a series of polls to inform the workshop design process.

1. What tools do you find most useful when working in maritime security?
(Tools can include things like websites, data analysis software, communication and situational awareness tools)
 - a. _____
 - b. _____
 - c. _____
2. At the workshop, we will analyze a specific tool for its effectiveness. What tool would you like to target for discussion?
 - ___HOMEPORT (USCG)
 - ___Informal networks (phone, emails)
 - ___Marine Exchange
 - ___MarView (MARAD)
 - ___Other (please specify): _____

MIST Poll #4: survey regarding useful organizations, conferences and meetings

1. What organizations or meetings do you find most useful when working in maritime security?
(Include things like associations, agencies, special interest groups, local events, conferences and workshops).
 - a. _____
 - b. _____
 - c. _____
2. Why are these organizations and meetings useful?

MIST Poll # 5: The final poll prior to the MIST Puget Sound Workshop to target tools to discuss as a group.

1. During the workshop we will be looking closely at a few *best of class* models for information sharing. Which would you like to target for discussion? (choose all that apply)
 - ☐ Area Maritime Security Council (AMSC)
 - ☐ Joint Harbor Operations Center (JHOC)
 - ☐ Joint Terrorism Task Force
 - ☐ Information Sharing and Analysis Center (ISAC)
 - ☐ Marine Exchange
 - ☐ Other (please specify)

Evaluation

Included in the MIST Puget Sound Workshop participation packets, attendees were encouraged to complete this one page, double-sided evaluation at the close of the second day.

MIST evaluation

1. Thank you for joining us for this MIST workshop

To help us improve the workshop, please tell us about your experience. Thanks!

* 1. Your organization is a:
(mark only one)

☐ Private company

☐ Public association

☐ Federal agency

☐ State or local agency

Other (please specify)

2. Overall, how well organized was this workshop?

☐ Very well organized ☐ Somewhat organized ☐ Somewhat disorganized ☐ Very disorganized

3. Overall, how useful was this workshop?

☐ Very useful ☐ Somewhat useful ☐ Not very useful ☐ Not at all useful

4. How effective were the individual sessions in helping identify issues with sharing information?

	Very effective	Somewhat effective	Not very effective	Not effective at all
Presentations	☐	☐	☐	☐
Small groups	☐	☐	☐	☐
Large groups	☐	☐	☐	☐

Comments

5. How appropriate were the topics we discussed? Check all that apply.

	Personally interesting	Applicable to my job	Not appropriate
Incentives for the private sector	☐	☐	☐
Streamlining government requests	☐	☐	☐
Tools for information sharing	☐	☐	☐
Private sector issues in information sharing	☐	☐	☐
Solutions for better information sharing	☐	☐	☐
Networking	☐	☐	☐

MIST evaluation

6. The workshop was:

	Agree	Somewhat agree	Somewhat disagree	Disagree
Too long	☐	☐	☐	☐
Too short	☐	☐	☐	☐
Made me feel rushed	☐	☐	☐	☐
Was too slow	☐	☐	☐	☐
Did not provide enough breaks	☐	☐	☐	☐

Comments

7. Were the right people in attendance to capture the needs of the private sector?

☐ Yes

☐ No

If no, who would you include?

8. How likely would you be to do the following:

	Very likely	Somewhat likely	Not very likely	Not likely at all
Read background information before the conference	☐	☐	☐	☐
Use the web site before the workshop	☐	☐	☐	☐
Use the web site after the workshop	☐	☐	☐	☐
Set up your personal profile on the web	☐	☐	☐	☐
Add a resource to the web site	☐	☐	☐	☐
Recommend this workshop to others	☐	☐	☐	☐
Continue to participate in information sharing activities like this	☐	☐	☐	☐

Comments

9. In future workshops, what would you have us do *MORE* of?

10. In future workshops, what would you have us do *LESS* of?

Follow up

MIST Poll # 6: This follow up poll seeks input as to how this process might better benefit participants.

1. Your roll in maritime security is: (select one)
 - ☐ Facility Operations
 - ☐ Vessel Operations
 - ☐ Law Enforcement
 - ☐ Shipper
 - ☐ Other (specify below)

2. Your organization is a: (select one)
 - ☐ Private company
 - ☐ Public association
 - ☐ Federal agency
 - ☐ State or local agency
 - ☐ Other (specify below)

3. One of the things we heard you say at the recent workshop was that you'd like a more tangible benefit in exchange for workshop participation. What type of post-event benefit would be most useful?
 - ☐ Summary document designed for inclusion with Port Security Grant applications
 - ☐ Official Letter of Participation from a federal level security official
 - ☐ Other (please specify)

4. For future workshop design, what training should be included to maximize the participant benefit?
 - ☐ Tools orientation/training (i.e. HOMEPOR, MarView, other internet resources)
 - ☐ Port Security Grant application tips from a federal level application reviewer
 - ☐ Labor/industry communication training by a labor communication specialist
 - ☐ Other (please specify)

5. For you, the most important issue discussed in the recent workshop was: (select one)
 - ☐ Coordination, communication, and streamlining
 - ☐ Incentives for threat information sharing
 - ☐ Partner organizations, agencies, and associations
 - ☐ Best practices, ideal system design
 - ☐ Other (please specify below)

Appendix D: List of acronyms

AAPA	American Association of Port Authorities
AIS	Authorized Identification System
AMSC	Area Maritime Security Committee
AWO	American Waterways Operators
BCO	beneficial cargo owner
CAPA	California Association of Port Authorities
CBP	Customs and Border Protection
COTP	Captain of the Port
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership against Terrorism
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DON	Department of the Navy
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FIST	USCG Field Intelligence Support Team
FOUO	for official use only
FSO	Facility Security Officer
GAO	Government Accountability Office
GMAII	Global Maritime and Air Intelligence Integration
GMISS	Global Maritime Information Sharing Symposium
GMSA	Global Maritime Situational Awareness
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IPSC	Infrastructure Protection Subcommittee
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
IT	Information Technology
JHOC	Joint Harbor Operations Center
JTTF	Joint Terrorism Task Force
LA/LB	Los Angeles/Long Beach
MARAD	Maritime Administration
MARLO	Maritime Liaison Office
MASTER	Maritime automatic tracking enhanced reporting system
MDA	Maritime Domain Awareness
MDSRP	Maritime Defense and Security Research Program
MIST	Maritime Information Sharing Taskforce
MSSIS	Maritime Safety and Security Information System
NCAGS	Naval Cooperation and Guidance for Shipping
NOAA	National Oceanic and Atmospheric Administration
NORAD	North American Aerospace Defense Command
NORTHCOM	United States Northern Command
NPS	Naval Post Graduate School
NSIS	Nation Strategy for Information Sharing
NSPD	National Security Presidential Directive
NSMS	National Strategy for Maritime Security

Appendices

NSPD	National Security Presidential Directive
NW WARN	Northwest Early Warning Network
NY/NJ	New York/New Jersey
OGMSA	Office of Global Maritime Situational Awareness
ONI	Office of Naval Intelligence
OSAC	Overseas Security Advisory Council
PMSA	Pacific Merchant Shipping Association
PNWER	Pacific Northwest Economic Region
TSCC	Transportation Sector Coordinating Council
TWIC	Transportation Worker Identification Credential
USCG	United States Coast Guard
WMD	Weapons of Mass Destruction
WPPA	Washington Public Port Association





Appendix E: References

- Clark, ADM Vern (2005). *Edited remarks from 1 February 2005: San Diego CA*. San Diego Union-Tribune Editorial Board. <http://www.navy.mil/navydata/cno/clark/speeches/clark050201-ed.txt> (accessed 6 June 2009).
- DON (2007). "A Cooperative Strategy for 21st Century Seapower." *A publication of the Department of the Navy, U.S. Marine Corps, and the USCG*, October 2007. <http://www.navy.mil/maritime/MaritimeStrategy.pdf> (accessed 15 April 2009).
- DHS (2002). *National Strategy for Homeland Security*. Washington, D.C.: GPO, July 2002.
- DHS (2004). "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." *The National Commission on Terrorist Attacks upon the United States*, Thomas H. Kean, Lee Hamilton., Published by W. W. Norton & Company, 2004. www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf (accessed 21 January 2007).
- DHS (2005). "Maritime Commerce Security Plan," part of *The National Strategy for Maritime Security*. October 2005. http://www.dhs.gov/xlibrary/assets/HSPD_MCSPlan.pdf (last accessed 29 June 2009).
- Fann Thomas, Gail, PhD., Dr. S. Page Hocevar, and Dr. E. Jansen (2006). *A Diagnostic Approach to Building Collaborative Capacity in an Interagency Context*. NPS Acquisition Research Sponsored Report Series, 25 September 2006.
- GAO (2002). *Homeland security: Management challenges facing federal leadership*: GAO-03-260. Washington, DC: December 2002.
- Intelligence Reform and Terrorism Prevention Act of 2004, 118 STAT. 3638 *Public Law 108-458—Dec. 17, 2004*. 50 U.S.C. 401 note. <http://travel.state.gov/pdf/irtpa2004.pdf> (accessed 29 June 2009).
- Mettruck, CPTN Steven (2009). "Leveraging People and Technology to Optimize Interagency Interoperability: The Puget Sound Joint Harbor Operations Center." *USCG Proceedings*, Spring 2009, 76-81.
- OGMSA (2008). "GMISS Findings and Recommendations: increasing industry/government maritime information sharing partnerships to the benefit of safety, security, commerce, and the environment." *Global Maritime Information Sharing Symposium*, August 2008. http://www.gmsa.gov/twiki/bin/view/Main/GMISS08Report?sortcol=table;up=#Need_for_New_Approaches (accessed 18 June 2009).
- Price, Willard (2004). "Reducing the Risk of Terror Events at Seaports." *Review of Policy Research* 21(3), 329-349.
- Renuart, Victor E., Jr., Dane S. Egli (2008). "Closing the capability gap: developing new solutions to counter maritime threats." *Naval War College Review*, Spring 2008, 61(2), 14-24.
- Salem, Anita; Wendy Walsh and Owen Dougherty (2008). "Industry and Public Sector Cooperation for Information Sharing: Ports of Long Beach and Los Angeles," a joint publication of the



- Naval Postgraduate School and the Maritime Administration*. September 2008.
<http://www.gmsa.gov/twiki/bin/view/Main/GMISS08Report?topic=MistSymposium>
(accessed 29 June 2009).
- Ulmann, R.E., Enlow, Yonsuk (2006). "Accelerating Technology Adoption Through Community Endorsement." *Geoscience and Remote Sensing Symposium, 2006*. IGARSS 2006.
- Wagner, Breanne (2007). "Reluctance to Share Information Hampers Counterterrorism Efforts." *National Defense Magazine*, September 2007. <http://www.nationaldefensemagazine.org/archive/2007/September/Pages/Reluctance2513.aspx> (accessed 19 June 2009).
- Walsh, W.B. (2009). "A Sea of Change for the Obama Administration: restructuring domestic maritime security to prevent attacks from the sea." *currently unpublished*, April 2009.
- The White House (2004). "Maritime Security Policy." *National Security Presidential Directive 41 / Homeland Security Presidential Directive 13*, 21 December 2004. http://www.dhs.gov/xprevprot/programs/editorial_0597.shtm (accessed 21 January 2007 and 23 March 2009).
- The White House; MSPCC (2005). *National Strategy for Maritime Security*, September 2005. http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf (last accessed 23 March 2009).
- The White House (2007). *The National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. <http://www.whitehouse.gov/nsc/infosharing/index.html> (accessed 12 September 2008).
- Wright Candice L. (2007). "Bridging the Gap in Port Security; Network Centric Theory Applied to Public/Private Collaboration." *Naval Postgraduate School, Monterey, CA*. March 2007.