2012-11

Multimodal Information Sharing Team

þÿ(MIST) Port of Baltimore Ind

Public Sector Cooperation for Information Sharing

NPS-GSBPP-13-001

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MIST
MULTIMODAL INFORMATION SHARING TEAM - PORT OF BALTIMORE INDUSTRY AND PUBLIC SECTOR COOPERATION FOR INFORMATION SHARING

by

Dr. Susan Hocevar, Wendy Walsh, Anita Salem, Lyla Englehorn

November 2012

Approved for public release; distribution is unlimited

Prepared for: Program Manager, Information Sharing Environment (PM-ISE)
2100 K Street, NW, Suite 4000
Washington, DC 20511

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	**2. REPORT TYPE**	**3. DATES COVERED** ***(From-To)***
01-Nov-2012	Technical Report	**May – 30 September 2012**

4. TITLE AND SUBTITLE

Multimodal Information Sharing Team (Mist) - Port Of Baltimore Industry and Public Sector Cooperation for Information Sharing

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Susan Page Hocevar, Wendy Walsh, Anita Salem, Lyla Englehorn

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-GSBPP-13-001

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Program Manager, Information Sharing Environment
ISE Mission Programs Division
2100 K Street, NW
Suite 4000
Washington, DC 20511

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

14. ABSTRACT

The Multimodal Information Sharing Team (MIST) is an evolution of the Maritime Information Sharing Taskforce that has been conducting workshops in domestic ports since 2008. The MIST provides a framework and process for the collaborative exploration of information sharing across the port multimodal community. The MIST emphasizes the private sector perspective to ensure that government stakeholders are leveraging this critical player in the sharing of all hazards threat information. The Program Manager for the Information Sharing Environment (PM-ISE) sponsored the Baltimore MIST. This report presents the results of an action planning workshop that involved over 30 local, state, and national public and private sector stakeholders in maritime security for the Port of Baltimore. It highlights the motivations for information sharing and the information needs of both public and private sector. It uses the Inter-Organizational Collaborative Capacity model to organize the analysis and recommendations for three aspects of information sharing: security-focused mechanisms, commerce-focused mechanisms, and technology mechanisms. The report concludes with a set of both immediate-term and long term actions that were identified by workshop participants. Through the MIST collaboration, the PM-ISE in partnership with National Maritime Intelligence-Integration Office (NMIO) will continue to work with the Baltimore area, supporting the on-going development of the Maritime Law Enforcement Information Network (MLEIN).

15. SUBJECT TERMS
Information Sharing; All-hazards Threat Information; Private Sector; Inter-Organizational Collaboration

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Susan Page Hocevar
Unclassified	Unclassified	Unclassified	UU	46	**19b. TELEPHONE NUMBER** ***(include area code)*** 831-656-2249

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RDML Jan E. Tighe
Interim President

O. Doug Moses
Acting Provost

The report entitled *"Multimodal Information Sharing Team (MIST) – Port of Baltimore Industry and Public Sector Cooperation for Information Sharing"* was prepared for and funded by the Program Manager, Information Sharing Environment (PM-ISE), 2100 K Street, NW, Suite 4000, Washington, DC 20511.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Dr. Susan Page Hocevar
Associate Professor

Wendy Walsh
Program Manager

Anita Salem
Research Associate

Lyla Englehorn
Research Associate

Reviewed by:

William R. Gates, Ph.D.
Dean, Graduate School of Business and Public Policy

Released by:

Jeffrey D. Paduan
Vice President and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Multimodal Information Sharing Team (MIST) is an evolution of the Maritime Information Sharing Taskforce that has been conducting workshops in domestic ports since 2008. The MIST provides a framework and process for the collaborative exploration of information sharing across the port multimodal community. The MIST emphasizes the private sector perspective to ensure that government stakeholders are leveraging this critical player in the sharing of all hazards threat information. The Program Manager for the Information Sharing Environment (PM-ISE) sponsored the Baltimore MIST. This report presents the results of an action planning workshop that involved over 30 local, state, and national public and private sector stakeholders in maritime security for the Port of Baltimore. It highlights the motivations for information sharing and the information needs of both public and private sector. It uses the Inter-Organizational Collaborative Capacity model to organize the analysis and recommendations for three aspects of information sharing: security-focused mechanisms, commerce-focused mechanisms, and technology mechanisms. The report concludes with a set of both immediate-term and long term actions that were identified by workshop participants. Through the MIST collaboration, the PM-ISE in partnership with National Maritime Intelligence-Integration Office (NMIO) will continue to work with the Baltimore area, supporting the on-going development of the Maritime Law Enforcement Information Network (MLEIN).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. Introduction 1

A. MIST Baltimore 1

B. Findings 2

1. Motivations 2

a. Financial & operational motivations 3

b. Strategic & ideological motivations 3

c. Social motivations 4

C. Information needs 4

1. Information quality 5

2. Information types 5

D. Inter-Organizational Collaborative Capacity 6

1. Leading and lagging factors 6

2. Common themes from small group discussions 6

3. Spotlight: Inter-Organizational Collaborative Capacity (ICC) 7

4. Small group report: Security focused mechanisms 8

5. Small group report: Commerce-focused mechanisms 10

6. Small group report: Technology mechanisms 13

E. Next Steps for Baltimore 16

Appendix A: Methods 17

Appendix B: List of acronyms 19

Appendix C: Baltimore Systems Guide 2012 20

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1: Stakeholder Motivations 3
Figure 2: Information needs 4
Figure 3: ICC Model 7

THIS PAGE INTENTIONALLY LEFT BLANK

I. Introduction

The Multimodal Information Sharing Team (MIST) is an evolution of the Maritime Information Sharing Taskforce that has been conducting workshops in domestic ports since 2008. The MIST provides a framework and process for the collaborative exploration of information sharing across the port multimodal community. The MIST emphasizes the private sector perspective to ensure that government stakeholders are leveraging this critical player in the sharing of all hazards threat information.

To date, MIST has held six events throughout the U.S. at the ports of Los Angeles/Long Beach, the Puget Sound, Honolulu, the Delaware Bay, Boston, and Baltimore. As we began this journey we heard the mantra, 'when you've seen one port, you've seen *one* port,' highlighting the uniqueness of each area. Yet, over time our research has shown that while the commodities and geography vary from port to port, the people are more alike than different when it comes to sharing information. Our earlier findings show that industry-government information sharing is improved by improving collaboration, increasing cultural awareness, improving communication tools, and aligning financial and non-monetary incentives with industry motivations.[1,2,3,4,5]

A. MIST Baltimore

There are a number of partners involved in the sharing of threat information in the Baltimore area (see Appendix for a full list.) As part of our process, MIST worked with some of these local partners to establish the goals and process for the workshop. Similar to other port environments, the Baltimore Maritime Exchange (BME) was of major assistance in this community. After a single call to the Director of the BME, we were invited to attend a hot-wash of a recent large event, Sailabration. During that time, we were able to begin to identify the appropriate workshop participants and see the strengths of the community.

As part of this early outreach, we discovered a local best practice in information sharing--the Maryland Law Enforcement Information Network (MLEIN). MLEIN is a multi-sensor, interagency information-sharing tool that is being put together under the leadership of the Maryland Department of Natural Resources (DNR). The time and resources invested in this effort were recognized as a good example of local collaboration in the development of a state-of-the-art interagency information sharing process. As part of the MIST process, we connected the developers of MLEIN with our Baltimore sponsor, the Program Manager, Information Sharing Environment (PM-ISE) (See Spotlight: ISE.) The result is that the PM-ISE is contributing to the continued development of the MLEIN tool. MLEIN will be released to stakeholders on December 31, 2012.

The MIST team conducted a follow-up visit and attended several standing meetings as well as met with stakeholder's one-on-one to learn more about the Baltimore Port community. Based on these meetings, we developed a local steering committee to ensure that we had good representation in the workshop. The steering committee consisted of active members from the BME, DNR and the Maryland Port Administration.

SPOTLIGHT: ISE

The Program Manager for the Information Sharing Environment (PM-ISE) sponsored the Baltimore MIST. The mission objectives of the PM-ISE are to:

- Advance responsible information sharing to further counterterrorism and homeland security missions
- Improve nationwide decision making by transforming information ownership to stewardship
- Promote partnerships across federal, state, local and tribal governments, the private sector and internationally

The conversations and recommendations at each MIST have embodied the PM-ISE objectives with a specific emphasis on the voice of private sector and most recently the multimodal community at large. We were fortunate to have representatives from PM-ISE at this workshop and look forward to continued collaboration.

We are very pleased that through the MIST collaboration, the PM-ISE in partnership with National Maritime Intelligence-Integration Office (NMIO) will continue to work with the Baltimore area, supporting the on-going development of the Maritime Law Enforcement Information Network (MLEIN). This is a clear demonstration of "cross-domain information integration in the pursuit of strengthening national security through responsible information sharing." (2012 ISE Annual Report to Congress)

B. Findings

The goals of the MIST workshops are to identify key issues in information sharing, engage participants in specific problem solving activities and address issues of most importance to local port security stakeholders. To achieve these goals, MIST worked with participants to: identify their motivations for sharing threat information; identify their challenges and needs in receiving quality information; and improve their ability to collaborate.

1. Motivations

Stakeholder motivations, both material and social, are important factors in the adoption of new processes, policies, and technologies to improve all-hazards threat information sharing. Understanding what motivates people to participate in information sharing is important because this understanding can be used to better align federal policies and processes. First, we can use the motivations to help us align federal incentives with stakeholder interests. Second, stakeholder motivations can be used to create strategic communication plans that utilize underlying industry support and address possible resistances to sharing threat information. For this reason, the MIST team has consistently explored private sector motivations to share information. To help better understand the motivations of this port, we presented our previous findings on motivations and asked participants to discuss the motivations of the Baltimore port partners. Using our previous model for evaluating motivations (see Figure 1), the group discussed their financial, operational, social, ideological, and strategic motivations.

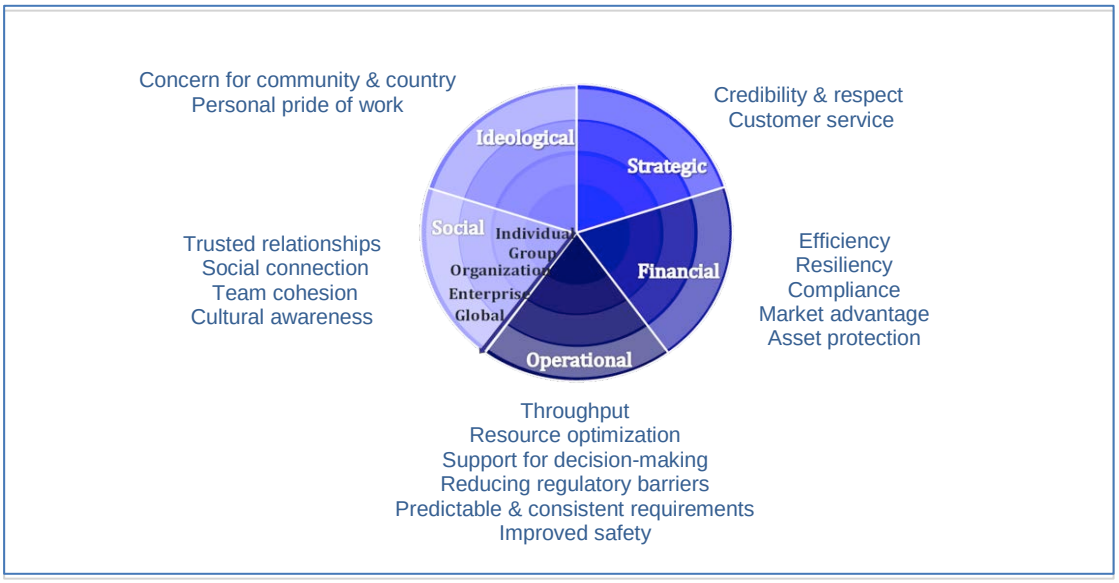

Figure 1: Stakeholder Motivations

a. Financial & operational motivations

"We need to ensure that commerce is not interrupted."

Financial motivations exist when there are opportunities for material benefits or monetary rewards. Operational motivations concern increased efficiency and effectiveness of the organization that lead ultimately to financial benefits. Our Baltimore participants identified several instances where information sharing benefited them financially or operationally and was seen as a valuable activity. One example was a recent three-port conference call during preparations for a hurricane. This pre-planning communication was viewed positively because it allowed all three ports to work together early on in order to mitigate the risks of port closures: "Historically, this would have happened with limited notification." A second example of coordinated operational planning was in the recent "1812 Sailabration" event. Because government agencies collaborated with the private sector from the beginning, industry was able to minimize the impact on commerce: "The private sector didn't miss a beat." The third example provided was current and involves a potential labor strike. Industry expressed a need for instituting security plans and communicating well: "If we don't know when, how big, where, what is the potential for violence, we may not get vehicles loaded…costing us $60K a day and not getting to the locale expecting them."

Useful Practice

For Baltimore, resiliency, asset protection, throughput, and predictability are strong motivators for sharing threat information.

b. Strategic & ideological motivations

"We need to persuade HQ of the value of building partnerships to improve corporate performance."

Strategic motivations are organizational or personal perspectives, plans, and patterns that are valued and used to further the success of the stakeholder or organization. Our Baltimore participants discussed the problem that corporate leadership often does not see the value of sharing information—security is just a "necessary evil." Local participants saw a need to build a commitment to security within industry. Some factors that were identified to increase this commitment are demonstrating the business benefits (e.g., cost mitigations) of investing in information sharing and security, communicating government regulations, utilizing grants, including information sharing activates in port security plans, and formalizing information sharing through a Facility Security Officer (FSO) subcommittee.

In Baltimore, private sector participants related their strategic benefits directly to financial and operational factors. There is not yet a strong connection between strategic goals and the need for information sharing.

c. Social motivations

"Opportunities for interaction build bridges and (strengthen) relationships."

Social motivations take into account the interests, intentions, or needs of people. In Baltimore, participants noted how the social interactions in Baltimore are generally very positive. For instance, the Quality Cargo Handling Action Team (QCHAT) meetings involve labor and Customs and Border Protection (CBP) is active in U.S. Coast Guard (USCG) meetings. The Area Maritime Security Committee (AMSC) and the Captain of the Port (COTP) are seen as two strong mechanisms for interaction and the group identified several areas for improvement. First because the private sector has a perception that there could be a negative regulatory response when sharing information, the USCG needs to balance their regulatory and collaboration roles. In addition, there is a need for increased transition planning so that new personnel are better oriented to the specifics of Baltimore. This planning needs to "include who the key partners are, how people should be involved, and what their expectations are."

As in all of our other ports, Baltimore identified the importance of building relationships when encouraging the private sector to share information.

C. Information needs

"We need methodologies for sharing information—we need access."

By understanding the specific information needs of the public and private sector, system designers can create information systems that meet the needs of their constituencies. Typically in system design, these requirements are operationalized into a set of performance and usability requirements. These requirements can then be used during design and testing to develop high quality information systems. In previous workshops we gathered data from the private sector on what makes a high quality information system. Three key factors emerged—accessible information, ease of use, and useful information (see Figure 2).

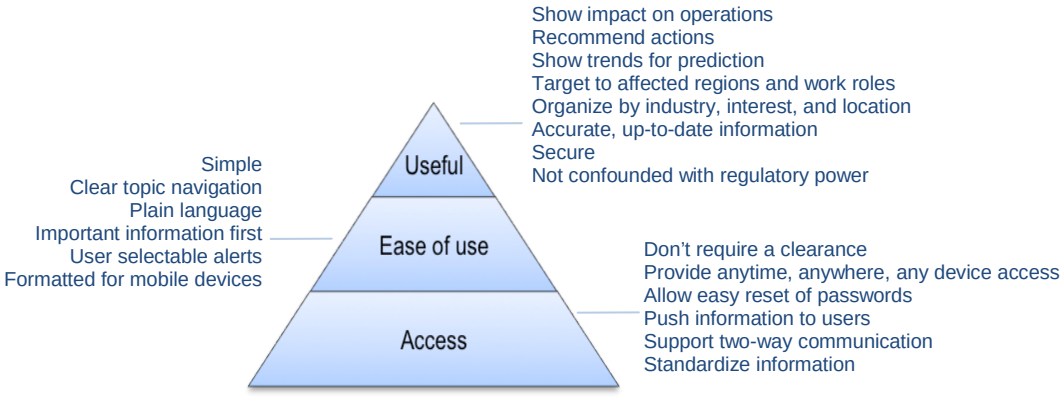

Figure 2: Information needs

During the workshop, we presented these findings and opened the discussion to identify local issues. Baltimore participants highlighted a number of challenges to getting high quality information:

1. Information quality

Accessible

- Limited awareness of what delivery systems are available
- Need for improved coordination between the USCG and the Maryland Coordination and Analysis Center (MCAC) in getting information to the private sector
- Difficulty getting "For Official Use Only" (FOUO) information because of certification or non-disclosure requirements
- Policy barriers preventing the sharing of active case files
- Password problems with Homeport
- A lack of feedback and follow-through on reports of suspicious activities
- Local law enforcement has limited capability to provide adequate two-way communications

Easy to Use

- Redundant information

2. Information types

Participants also identified the types of information that are needed in order to help them to be more observant, take preventive action, and maintain efficient operations:

Actionable

- Clearance lists for pilots
- Notices of Arrival
- Regulatory changes
- Contingency planning

Targeted

- Anything that could impede the movement of traffic
- Maritime related thefts
- Drug smuggling activities
- Human trafficking

Credible

- Complete information

Participants also noted areas where information sharing is effective:

- Monthly meetings and digests used by the cruise line industry
- USCG's sharing of information about the recent movements of a Greenpeace ship
- Maritime Exchange system for pushing out information

D. Inter-Organizational Collaborative Capacity

The MIST workshop facilitators introduced the Inter-Organizational Collaborative Capacity (ICC) model as a way to help local participants diagnose current collaborations and identify improvements to enhance all-hazards information sharing. (See "Spotlight: Inter-Organizational Collaborative Capacity (ICC)"). Prior to the workshop, a brief ICC survey was distributed to participants as part of a pre-workshop poll. The results of that poll were presented during the workshop to explain the model and initiate a discussion of collaboration issues across stakeholders in the Port of Baltimore. The pre-poll data highlighted some "leading" and "lagging" factors impacting collaboration in information sharing.

1. Leading and lagging factors

The strongest "leading" factor identified in the pre-poll was the shared recognition of the need for effective information sharing for security of operations for the Port of Baltimore. Other highly rated questions concerned existing capabilities and areas targeted for improvement. For example, one of the highest rated items demonstrated the benefits of the existing social and professional networks– people generally know whom to contact in public and private organizations regarding all-hazards threat information. But, further investigation showed that this awareness is not complete, and that points of contact frequently change (particularly in public agencies).

Several lower-rated, or "lagging" factors were also identified from the pre-poll data. These areas indicate where specific improvements may be merited. For example, participants questioned the adequacy of budgets and resources for effective all-hazards threat information sharing. Participants identified four other improvements:

1. to increase the clarity of roles and responsibilities
2. to place a greater emphasis on rewarding personnel for engaging in inter-organizational collaborations to improve information sharing
3. to increase opportunities for training and exercises involving all multimodal participants
4. to establish criteria for evaluating the success of information sharing efforts.

2. Common themes from small group discussions

Following the whole-group discussion summarized above, the participants divided into three groups to further examine what is currently happening in all-hazards information sharing and to identify specific desired improvements for public and private stakeholders in the Port of Baltimore. Each of the three groups focused on different current collaborative mechanisms for information sharing that had been identified in preliminary site interviews. The three groups were:

1. Security-focused mechanisms
2. Commerce-focused mechanisms
3. Technology mechanisms

Several of the themes that emerged from the small group discussions reinforced the pre-poll findings. For example, all groups acknowledged the strong culture of collaboration and existing information-sharing mechanisms in the Port of Baltimore. However, all three groups also identified the need to broaden the maritime-focus to include all multimodal partners and specifically called for strengthening the engagements with FSOs. The groups also identified limited resources as a key challenge, and recommended more pooling of resources, standardizing practices, and increasing efficiencies (e.g., improving access, reducing duplication).

3. Spotlight: Inter-Organizational Collaborative Capacity (ICC)

The Inter-Organizational Collaborative Capacity (ICC) model was originally developed in the context of US homeland security organizations to identify factors that enable and inhibit inter-organizational collaboration. A key assumption of this model is that building collaborative capacity requires deliberate leadership attention and the alignment of organizational design elements toward collaboration. As shown in Figure 4, the ICC model assesses five organizational domains: Purpose and Strategy, Structure, Rewards and Incentives, People, and Lateral Mechanisms. These domains include thirteen factors.

Purpose and Strategy.
The ICC model has three factors in the domain of Purpose and Strategy: (1) *Felt Need* is the recognition of interdependence with others and the acknowledged need to collaborate to effectively accomplish missions and goals. Felt Need often comes from perceptions of a shared challenge or opportunity. (2) *Strategic Actions* include goals for collaboration, demonstrated senior leadership commitment, and willingness to consider other organizations' interests in planning. (3) *Resource Investments* (e.g., budget, personnel) addresses the degree that investments are made to enable effective collaboration.

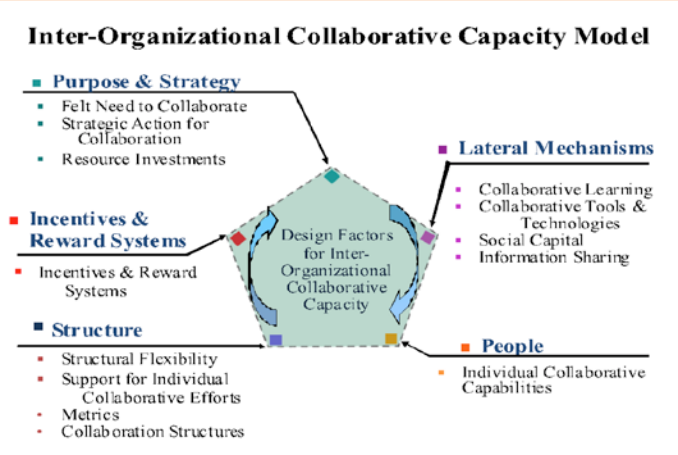

Figure 3: ICC Model

Structure
This domain comprises four factors. (1) *Collaboration Structures* can include liaison roles, participation in inter-organizational teams, clearly established roles for each participating organization, and internal processes that enable effective inter-organizational collaboration. (2) *Structural Flexibility* allows adaptation of partnerships as needs change, and demonstrates willingness to adjust procedures to facilitate coordination. (3) *Metrics* include established criteria and performance standards for evaluating inter-organizational efforts and assessing outcomes. (4) *Support for Individual Collaboration Efforts* has two facets. The first is how clearly individual collaborative work is structured in terms of goals, constraints, and authorities. The second is the strength of the link between personnel in boundary-spanning roles working directly with other organizations, and the strategic leadership of their own organization.

Incentives and Reward Systems
The original focus of this domain was on how *Reward Systems* impact personnel's willingness to collaborate. Are employees rewarded for investing time in building collaborative relationships or contributing to successful collaborative results? Are, collaborative talents and achievements considered when people are reviewed for promotion? A newer interpretation considers the motivation for organizations to engage in collaboration based on mandated requirements or grant opportunities.

Lateral Mechanisms
Four factors constitute this domain and represent the "hard" and the "soft" aspects of coordination. (1) *Social Capital* represents the social and professional relationships that organizational members have with counterparts in other organizations. It is a basis for awareness and trust-building. (2) *Collaborative Tools and Technologies* are the technical mechanisms for collaboration (e.g. inter-operable information systems and collaborative planning tools.) (3) The *Information Sharing* factor represents the organization's norms, values, and access that support information sharing. (4) *Collaborative Learning* is demonstrated through: cross-organizational training, learning about the capabilities of other organizations, and systematic assessment of lessons learned to improve future collaborations.

People.
This domain has only a single factor, *Individual Collaborative Capabilities*. These include the attitudes, skills, knowledge, and behaviors of individual organizational members that impact the organization's ability to collaborate. Examples are conflict management skills, willingness to engage in shared decision-making, respect for the expertise of those in other organizations, and knowledge and understanding of how other organizations work. [6,7]

Another common challenge was that the existing committees and organizations are "stove-piped" with a specific information-sharing focus (e.g., security information, commerce, maritime). Two groups discussed ways to expand these existing capabilities and one group explored the alternative of a new mechanism that would be more broad-spectrum to address multimodal, all-hazards information sharing needs. Related to the stove-piping is the need for improved communication planning to assist in broadening outreach. This planning needs to be based on an assessment of requirements and capabilities, and include specific plans for continuity of operations in the face of a system failure.

Finally, two of the groups raised issues with information technology and information access. For example, participants discussed the difficulties in updating passwords, having to use multiple sites to get a complete "picture" and seeing information that was not up-to-date. At the same time, groups also discussed the potential value of web-based technologies (e.g., webinars) for increasing interaction opportunities. A reoccurring theme was the importance of increasing opportunities for training. Groups discussed the need for better individual-level training (for information "consumers" and web-site managers) and the need for multimodal cross-organization training and exercises.

4. Small group report: Security focused mechanisms

The breakout group tasked with evaluating and recommending improvements to existing security information mechanisms in Baltimore found that the existing systems did not fully address their needs and recommended a new mechanism for sharing threat information. The final recommendation was for an all hazard, multimodal information sharing system that has a strong focus on operations as well as security.

The barriers and requirements for this new system are discussed below.

Current environment

The group began their discussion by identifying key information sharing mechanisms for the Port of Baltimore that stemmed from a security perspective. These mechanisms included both local and national technical systems and organizations:

- Area Maritime Security Committee (AMSC)
- Maryland Joint Operations Center (MJOC)
- Maryland Coordination and Analysis Center (MCAC)
- Homeport
- WatchKeeper
- Homeland Security Information Network (HSIN)

The group then looked in detail at existing and potential systems based on the five collaboration factors presented in the workshop.

Purpose and Strategy

Create an ongoing, 'all hazard' IT system that supports operations and security

The desired state for this group was to have an 'All Hazards' information system that is designed for *ongoing* communication (not only event triggered) and is focused on multimodal operations in the port. This information system should deliver actionable information that aids in decision-making. During the discussions, the break out group identified several areas where the desired strategic direction was out of alignment with existing systems in Baltimore.

First, even though the USCG has responsibility for three key information sharing systems (AMSC, Homeport, and WatchKeeper) participants felt that the USCG had a number of challenges in supporting the end-state described above. The first challenge is the USCG's exclusive focus on maritime—for the participants, a system needs to consider threats across the supply chain including multimodal partners such as trucking, rail, and pipeline. In addition, participants felt that the USCG, although active partners in information sharing, had limited financial and human resources to support all of their information sharing systems.

Second, the group felt that the HSIN, Homeport, MJOC, and MCAC were not appropriate mechanisms for industry because of their over emphasis on crime: "MCAC, DHS, and the MJOC are reactive to specific crime data and not focused on trends." In addition, this group felt that these mechanisms were weak in the maritime environment. The breakout group did, however, believe that there were many lessons to be learned from these other endeavors and that any new initiative should include input from those involved in existing mechanisms. In addition, the participants felt that the Maryland Maritime Strategic Security Plan provided a good foundation for future efforts.

Key challenges that were identified included the lack of adequate funding and the need for appropriately skilled human resources.

Recommendations

- Create an *ongoing* process for the sharing of 'all hazard' threat information.
- Focus on how security impacts port operations.
- Deliver actionable information that aids in operational decision-making.
- Address funding and resource needs.

Structure
Expand existing maritime structures, then expand to multimodal

The breakout group also discussed the supporting structures that were available to assist the start up of a new information sharing system. The consensus was that it would be best to start with the maritime community in order to leverage existing interest and resources and then quickly expand to include multimodal partners. The group first identified the need to have direct communication with FSO's and recommended developing an FSO subcommittee for the AMSC. The group also would like to create a core group to design the organizational roles and responsibilities of the new information sharing system. Finally, the group identified two existing initiatives that could be used to support an information sharing process. Both the USCG's AMSC and virtual IOC concepts were identified as possible supporting structures for a new information sharing process.

Recommendations

- Expand existing maritime structures (AMSC, IOC), then expand to multimodal.
- Create an FSO subcommittee for the AMSC.
- Create a steering committee to develop a plan.

Lateral Mechanisms
Utilize technology to create a live, dynamic meeting environment

From the outset, this breakout group felt that existing mechanisms were not adequate or appropriate for the sharing of operations related threat information. Therefore, the primary focus was in creating a mechanism that allows participants to engage with each other regularly in live discussions of operational security. Participants suggested virtual meetings, such as webinars, as a key delivery requirement. The meetings should be able to be accessed through mobile devices, allow virtual voting on issues, and provide an opportunity for immediate responses. The group recognized that this would require dedicated resources and some kind of electronic, web based portal for access. Neither HSIN) nor Homeport were seen as viable options for this system.

Recommendations

- Create a 'virtual' meeting process.
- Provide a mechanism for live interaction and voting on issues.
- Identify an appropriate delivery system.

People
Include intermodal partners, with clear roles and responsibilities

For the group participants, any information sharing process must include intermodal partners from the Baltimore area. Participants felt that there were several groups in the Baltimore area that were already active and should be leveraged in the design of the new system. The group also felt that the information sharing mechanism should include rotating leadership from intermodal partners. Eventually, the mechanism will also require formal Memoranda of Understanding (MOU's.)

Recommendations

- Include intermodal partners.
- Utilize existing partnerships (e.g. FSO's, MCAC, USCG, JTTF, MDOT).
- Clarify partner roles and responsibilities.

Incentives
Demonstrate the value of an information system to agency & industry leadership

The group identified the importance of getting support from local leadership and of generating a broader interest locally in the concept of a multimodal, all-hazard system. The MCAC, the Joint Terrorism Task Force (JTTF), USCG, and CBP were identified as key agencies. Participants identified incentives that would help build this support:

Regulatory incentives

- Enhanced compliance and focused enforcement efforts (CBP)
- Fewer violations (USCG)
- Stronger criminal investigations (FBI)

Commercial incentives

- Improve professional training
- Protect people and assets
- Minimal impact on commerce

Social incentives

- Long lasting relationships
- Better working relationships
- Stronger relationship with USCG

Security incentives

- Increased situational awareness
- Strengthen security posture

Recommendations

- Build support from the rank and file and local leadership
- Emphasize regulatory, commercial, social, and security benefits

5. Small group report: Commerce-focused mechanisms

The breakout group that took on analyzing and recommending improvements to mechanisms focused on commercial operations called for more effective information sharing mechanisms, a greater engagement and commitment to information sharing by stakeholders, a strengthening of liaison roles, and improved communication plans.

Current Environment

Several mechanisms for commerce-focused information sharing exist in the Baltimore Port area. QCHAT, the Maryland Motor Truck Association (MMTA), and the BME were identified as organizations that the private sector relies on for information that affects commerce. BME also plays a key role as a conduit for relevant

information from public agencies to the private sector. One of the limiting factors in this capability is the lack of a method to push information from the public agencies to BME. Additional committees and organizations such as AMSC and the Baltimore Port Alliance (BPA) were identified as having "unrealized potential" in terms of all hazards information sharing across public and private stakeholders in the Port of Baltimore. The approach of this group was to address ways in which existing mechanisms (particularly those that provide commerce-focused information) could be enhanced to better share all-hazards information with all relevant port stakeholders.

Purpose and Strategy
Engage all relevant stakeholders.

The first strategic issue that this group addressed was how to engage key stakeholders. For example, it was identified that the liquid bulk, private terminal operators, rail and trucking groups are not adequately involved in information sharing with public and private stakeholders in port security. The group identified that it would be desirable to improve the involvement of these key groups.

The second strategic issue was on how to increase the commercial sector's investment in improved security and information sharing. The current assessment was that there are, in general, inadequate resources for security, hazardous materials safety, etc. Investments by private sector organizations primarily occur as a result of regulatory reviews (e.g., by USCG) rather than being considered from a facility-level business planning perspective. Maintaining cost-competitiveness is another major barrier to these investments. Participants also identified the potential benefits of pooling efforts and resources, and utilizing port security grants.

Recommendations:

Three specific recommendations derived from this discussion:

- Conduct outreach to engage multimodal stakeholders in discussions and action-planning.
- Increase commercial organizations' awareness of the risk/cost implications of possible threats:
  - Integrate threat-assessments (and related cost analyses) into facility-level business planning.
  - Use internal or external "audits" to identify risk-mitigation investments. Possible sources for these audits included insurance companies that could identify mitigation investments that would decrease insurance rates; or the FBI's maritime liaison.
  - Identify appropriate cost-sharing mechanisms to off-set private sector investments.
- Increase benefits of limited resources by pooling across stakeholder groups.

Structure
Provide adequate liaison roles and taskforces/committees.

This workgroup identified three primary structural limitations. The first was the lack of commercial representation at the MCAC fusion center. The second was that there is no existing structure that brings together FSOs and thus a missed opportunity for communicating, sharing best practices, training, etc.) The third and most significant discussion within the group was in identifying the critical role of the BME in information sharing. While acknowledging BME's value, the focus was on the potential consequences of the "single point of failure" in relying on that "node" in the network of port stakeholders. A related discussion was that current staff and budget limitations of BME also limit the potential value it could offer.

The group also discussed the importance of developing a communication plan that would accomplish a number of goals related to the analysis above. The group recommended that this plan be informed by an analysis of information requirements and existing mechanisms. The 2012 National Maritime Security Advisory

Committee (NMSAC) report on the information gaps that have been identified by commercial industry could be a starting point for this analysis*. The AMSC Incident Management Plan should be reviewed and updated to identify a public information service "back-up" to BME. There are also existing AMSC communication plans from other regions that might provide useful models. The group identified key organizations that should be involved in developing this plan, to include MCAC, USCG, AMSC, and the Maryland Port Admin-istration (MPA).

Recommendations

- MCAC should make a presentation to the BPA and identify ways to increase liaison with the private sector.
- Establish an FSO subcommittee to the AMSC and reinstate the current AMSC sub-committees to address improvements in information sharing.
- Develop a communication plan involving MCAC, USCG, AMSC, Law Enforcement, and MPA for information sharing across port stakeholders, to include analysis of information requirements, existing mechanisms, gaps, and contingencies.

Lateral Mechanisms
Improve the utilization of existing information-sharing mechanisms.

This working group identified several existing lateral mechanisms for information sharing where the commercial sector is engaged and some ways that lateral mechanisms could be improved. The QCHAT meets regularly bringing together the Maryland Port Administration, steamship lines, terminal operators, labor union and trade associations to exchange information that impacts business development and customer satisfaction. They discussed the benefits of having increased involvement of private terminals in addressing all-hazards threat information sharing and proposed the best vehicle for that would be through the BPA.

Another existing mechanism for information sharing is the Baltimore Maritime Exchange (BME) that had been identified in the discussion of structures as a central node in the system of stakeholders with interest in maintaining the free flow of commerce through the Port of Baltimore. The group felt that this organization could be better utilized as an information conduit if more organizations pushed information to BME who could then further disseminate. BME and USCG have a positive relationship, but there are currently limits on what government agencies can share and there has been limited use of the USCG Alert and Warning System (AWS). It was also recommended that quick response all-hazards (including Port events) information sharing sheets be developed that indicate what the information is, who the information goes to, etc.

A third lateral mechanism identified by the group is the AMSC. The working group expressed that there has been a decline in attendance in the AMSC and the sub-committees are currently not very active. This mechanism offers a key vehicle for addressing some of the recommendations listed in the sections above. The group also recommended that the AMSC meeting minutes be distributed to the full port community to try to increase involvement.

A final observation made by this group was that point of contact (POC) lists routinely become out-of-date. Addressing this problem should be part of the development of the communications plan identified in the discussion of structure above. One option is to develop information dissemination systems that are linked to organizational roles rather than specific individuals.

Recommendations

- Use the up-coming local discussions of environmental issues (e.g., watershed management) to increase engagement of private terminal operators.

* Note: The NMSAC report is based in large part on previous MIST findings.

- Increase "public service" information pushed from government agencies through BME to port stakeholders to improve commercial sector's ability to mitigate "bumps" in the flow of commerce.
- Distribute AMSC minutes to full port community of port stakeholders.
- Develop all-hazards, quick-response information sheets to facilitate timely distribution of information to all relevant multimodal port stakeholders.

People

Increase the general workforce commitment to all-hazards threat information sharing.

The majority of this working group's time was spent on the three topics described above. However, the group did identify the challenge of maintaining awareness among operational personnel about what information should be shared and with whom. They also discussed the need to increase the front line workers' "ownership" of the importance of port safety/security and their role in maintaining it. The establishment of an FSO sub-committee in AMSC can be a vehicle for regular training and USCG security briefings. The group also identified the opportunity of using BME and BPA websites to distribute port newsletters and highlight reports related to safety/security.

Recommendations

- Deliver regular, annual training to FSOs related to all-hazards information sharing.
- Use recommended FSO subcommittee of AMSC as vehicle for increased security briefings (e.g., from USCG) with FSOs.
- Use BME and BPA web presence to maintain awareness of safety/security issues among port workforce.

6. Small group report: Technology mechanisms

The breakout group concerned with the use of technology identified a number of areas where the use of technology could be improved. Group members called for better coordination, mitigation of the risk of technology failures, providing a single node information system, providing training in technology, and strengthening existing best practices.

Current Environment and Systems

The breakout group felt that currently the Baltimore multimodal community operates in an all hazards environment and when applicable develops technologies that can support all hazards information sharing.

There are several cross agency technology information sharing systems and tools that are used daily. However, the segmentation of these systems can be problematic. Private sector operators in Baltimore report interfacing with 6-7 systems per day while one public agency reported interfacing with more than 18 some days. These collaborative systems include: Homeport, HSIN, Google Alerts, VidSys video system, and WatchKeeper, a new Coast Guard information system. Still, with all the technology available, they report that the best way to build social capital remains face-to-face meetings as well coordinating on exercises and real-world events. This group reported that *people* are the heart of information sharing. Investing in people is investing in information sharing. Information sharing investment must include training and job experience to improve core competencies.

With better information sharing, it is anticipated that operations will require less time on the phone and less man-hours looking things up. This community expressed that organizational efficiency is a key incentive. They are also inspired to work together because of a common mission. They believe that sharing information results in a force multiplying effect. While there may be only one person in the agency focused on information security, working with others in the community expands each organization's reach.

Purpose and Strategy
Coordinate efforts and standardize

Strategically they are still working across the industry and the interagency to develop and actualize common goals. The Security Risk Management Plan and Maryland Maritime Strategic Security Plan are currently being updated for consistency. The outcome they are striving for is to have common and understood goals and visions. Strategically the community feels that pooling resources, standardizing approaches and coordinating efforts will be the most successful approach to achieve technology to support information sharing. The greatest barriers to achieving these efforts have been manpower, leadership, coordinated political support and a lack of private sector engagement.

While the individual agencies in Baltimore may not have specific goals for information sharing, it is supported in their mission statements and they are aligned with the Maryland Maritime Security Strategic Plan. Information sharing is valuable and this is demonstrated by agencies investing resources (time, money and people) to build technological capability to support information sharing across agencies and industry. One example of this is the Maryland Pilots who have increased server space to accommodate additional storage and sharing ability. Another example is the Maryland Natural Resources Police and the Department of Natural Resources who have been working over the past several years to pull together various technologies such as cameras, radar and video to provide data to MLEIN that supports the whole community in information sharing. MLEIN is designed to support search and rescue as well as environmental conservation response.

Recommendations:

- Continue to update existing plans for consistency in goals and vision across agencies.

Structure
Develop a continuity plan to mitigate technology failures

Structurally, the community has good relationships and an abundance of sources for information, but they do not have metrics for cross- agency collaboration and many times they have not established metrics for collaboration within their individual agencies. It was reported that they currently have some problems with information overload and the inappropriate use of the incident command systems has complicated communication and planning. The desired outcome conveyed is one where the planning process is streamlined and seamlessly integrates with individual organizational doctrine. They also conveyed desire to ensure that communication and information sharing systems do not fail when technology fails.

They reported that while they currently do not have formalized structures for measuring the impact of information sharing, they have captured indicators, such as complaints, website hits and lessons learned in exercises and actual event response.

Recommendations:

- Develop a multimodal Continuity of Operations Plan for information sharing when technology fails.
- Come to consensus on metrics for continuous improvement of information sharing across the multimodal community.

Lateral Mechanisms
Provide a single node for community-wide information sharing

The community of Baltimore does leverage lateral mechanisms to collaborate toward better information sharing. They demonstrate a strong culture of collaboration when planning for large events, such as the recent "1812 Sailabration." They also have engaged in some exercises that involve a broad range of stakeholders

including the private sector. One example is the I-STEP exercise that was scheduled two weeks after this MIST workshop. They also have fairly good mechanisms for sharing after action reports (AARs) to participants at follow on briefs. The shortcoming of these efforts is that some stakeholders still remain out of the loop and are unaware

of upcoming exercises and ways to engage in event planning. Outreach and communication are key to remedying this and social networking technology may assist in this. Unfortunately, leadership is also needed as many agencies and some organizations restrict access to social networking websites.

The group attested that the number of existing committees to promote information sharing and the strength of organizations such as the BME clearly demonstrate the commitment of the people to engage. However, they agreed that lateral mechanisms are limited by the lack of a single sign on or website portal for information sharing. Users are required to have a multitude of passwords to work across agencies and organizations. One participant brought in a large file folder he uses to track the website and passwords he needs for sharing and receiving critical operational and security information. While there is a strong culture of working together there is not a business practice or orientation for sharing information and the community currently lacks a single node for community-wide information sharing.

Recommendations:

- Identify a single node for information sharing
- Facilitate linking information sharing websites to reduce the number of passwords needed to access critical information

People

Provide training so that people can effectively interface with the collaboration systems

This workgroup identified one major element that may be hampering the intention of the community and that is training. Participants shared that people are not always trained to interface effectively with the systems that are intended to connect them, whether that be web sites or radios. Training needs to be made available; it is important that the community does not assume that all stakeholders have basic aptitude to leverage information sharing technologies fully. Last, but not least, people need to have access to relevant training to utilize various interagency information sharing technologies.

Recommendations:

- Provide regular trainings for stakeholders to learn about and gain skills in using the information sharing technologies available.

Incentives

Recognize that risk is reduced by enabling information sharing

The technology group felt that collaboration in Baltimore has proven to save time and improve security, which makes it all worthwhile. Further emphasizing incentives for information sharing, they conveyed that it also helps them to achieve their individual agency and organizational missions. The more they have opportunities to collaborate the better they understand each other. They believe the breakdown of stove piped information systems will result in better coordination for planning, response and recovery. Participants expressed that this coordination can be realized through valuing and repeating information sharing best practices and this will take leadership, both in government and private industry, to recognize that in enabling information sharing we will reduce risk. The challenge is in adequate manpower, clear communication and agreement that there is actual return on investment.

Recommendations:

- Provide a mechanism for sharing best practices in information sharing across the multimodal information sharing community.
- Create a strategy for executive level support of information sharing across the community.

E. Next Steps for Baltimore

In the closing hours of the Baltimore MIST workshop, each of the small groups presented a summary of their discussions with an emphasis on desired improvements, recommendations, and specific action steps. A detailed list of both immediate-term and longer-term actions were posted on the walls and participants were asked to "sign up" indicating if they (or their organization) would take a leading/facilitating role on the activity, or be part of the group to more fully develop the action idea and identify specific implementation steps. These recommendations, and the roles participating organizations volunteered to play, are listed in the Table below (details on the activities are described in the group breakout discussions above.)

Table 1: Next Steps

Activity	Lead	Team
Develop an info sharing mechanism and matrix to capture efforts & resources across all stakeholders determining who has what and how distributed-	AMPorts	BME (additional team members needed for this task)
Identify data and information sharing tools that could be used in the new 'cloud' environment	DNR	MCAC, MEMA, DoD-MDA, NMIO & USCG
Develop an information sharing communications plan that is all-hazards and includes all multimodal stakeholders that articulates problem statement and business planning implications for information sharing and strategies to develop executive-level support.	BME, MPA, AMPorts & Vane Bros	USCG, USCG-HQ-IOC, MTA, SPIMAC, MSP/MCAC
Establish FSO subcommittee	USCG	AMPorts, Dominion Cove Point
Develop a process to distribute AMSC minutes to port stakeholders	USCG	BME
Build information sharing into security plans and develop quick response all-hazards info sharing sheets (including events) indicating what info is, who info goes to…)	USCG	AMPorts, BME & FSO community
Develop Intel Briefings	FBI	USCG
Ensure the multimodal community is included in activities	AMPorts	BME
Conduct external audits to identify threat assessments and risk mitigations	FBI & MCAC	USCG & PSA
Include a private sector representative in the MCAC	DHS/HSI	BME, AMPORTS, Van Bros & Ports America
Convey the risk & vulnerabilities of reliance on the BME as the critical information node	BME	MSP/MCAC/CIP, AMPorts & Pilots Association
Establish a mechanism to sustain the efforts of the MIST workshop	USCG	MPA
Use BME & BPA to distribute newsletters	BME	TBD
USCG	USCG-HQ, BME & BPA	

Appendix A: Methods

Using an iterative and participatory approach, MIST researchers partnered with federal, local and private sector stakeholders to assess the information sharing needs of regional multimodal security personnel. The resulting research design included site visits with interviews and participant observation of committee meetings; information sharing issues workshop; and informal polling.

Purpose

The mission of MIST *is to create a process for interagency and international multilateral sharing of multimodal threat infor-mation between the private sector and government agencies. This process must mitigate the concerns of private industry and provide value to both parties.*

Participant recruiting

Workshop and field study participants were invited to join the MIST efforts based on the recommendations of the local steering committee. The steering committee consisted of three active members form the BME, DNR and the Maryland Port Authority. There were also members from the USCG and FBI who were included in committee activities as available. The steering committee was very successful in getting a fairly good representation of the community, but as in other MIST workshops, we would have liked to have greater representation from the trucking and rail communities.

Invitations were sent out via the steering committee and followed up on by the NPS research team. Once an individual agreed to attend the workshop, they were included in a pre-workshop poll to gather data about current information sharing practices, challenges, and indicators of community collaboration capacity.

Participants included representatives from the following organizations:

Industry

- AMPorts
- Association of Maryland Pilots
- Baltimore Maritime Exchange
- CNX Marine Terminals Inc.
- Constellation Energy
- Dominion Cove Point
- Ports America
- Vane Line Bunkering

Government

- Customs and Border Protection (CBP)
- Department of Homeland Security (DHS) Private Sector Office
- Federal Bureau of Investigation (FBI) Baltimore
- Homeland Security Investigations – Immigration and Customs Enforcement (HSI – ICE)
- Information Sharing Environment (ISE)
- Maryland Port Administration
- Maryland Coordination and Analysis Center (MCAC)
- Maryland Natural Resource Police
- Maryland State Police
- Maryland Transit Administration
- Maryland Emergency Management Agency (MEMA)
- National Maritime Intelligence-Integration Office (NMIO)
- USCG Interagency Operations Centers (IOC)
- USCG Headquarters
- USCG Sector Baltimore

Workshop
The workshop was conducted over a day and a half and included large group discussions, breakout sessions, and action planning to improve multimodal, all-hazards information sharing. The workshop was segmented into several primary areas:

Why Share – Incentives for information sharing
In this section, participants were presented a summary of previous MIST findings. They then discussed local motivations for information sharing related to ideological, social, strategic, operational, and financial incentives.

What is shared – Exploring information sharing needs
Participants examined information sharing needs related to previous MIST findings. Building upon their information sharing needs, participants identified specific types of information that were relevant to know and share.

Who is key – Mapping how information is shared
By exploring stakeholder involvement in information sharing, participants examined their current information channels to prioritize key relationships and interactions related to information sharing.
How can we share – Collaborations and requirements

Following the whole-group discussion outlined above, the participants divided into three groups to further examine what is currently happening in all-hazards information sharing for public and private stakeholders in the Port of Baltimore and to identify specific desired improvements. Each of the three groups focused on different current collaborative mechanisms for information sharing that had been identified in preliminary site interviews. The three groups were:

1) Security-focused mechanisms
2) Commerce-focused mechanisms
3) Technology mechanisms

The small group activity was structured around a traditional change planning model. They were asked to assess the "current state" of all-hazards, public/private sector information sharing and to identify a more ideal or desired "end state." Groups were also asked to identify any relevant barriers or enablers to achieving the improvements identified. To give the discussion focus, groups were encouraged to use the ICC model to organize their discussion. This also facilitated comparison and integration of the results produced by the three groups.

Facilitators asked the workshop participants to choose which group they wanted to work with; but to also aim for a balance and diverse representation. Each group had from 8-12 members representing government (local and national) and private sector organizations. The groups worked for about 3 hours to assess current collaborative practices in their focal area and identify potential improvements. At the end of the day, participants were given a homework assignment – to return the following morning with specific action recommendations they would propose for achieving the improvements identified in the group discussions.

Next Steps
The final activity for the workshop was to discuss how participants could take action in information sharing best practices within their local area of responsibility. For the first 45 minutes of the second morning, participants reconvened in their small groups to review the prior day's discussions and share recommendations for action. Following this review, the plenary session rejoined and each group presented a summary of their work from the prior afternoon. After the summaries, participants outlined the next steps for moving forward and participants volunteered in their area of interest.

Workshop slides
The slide presentation used to structure the MIST workshop is available upon request. Please contact Anita Salem at amsalem@nps.edu

Appendix B: List of acronyms

AMSC	Area Maritime Security Committee
BME	Baltimore Maritime Exchange
BPA	Baltimore Port Alliance
CBP	U.S. Customs and Border Protection
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
DNR	Department of Natural Resources
FAA	U.S. Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GMAII	Global Maritime and Air Intelligence Integration -
HSI-ICE	Homeland Security Investigations – U.S. Immigration and Customs Enforcement
ICE	U.S. Immigration and Customs Enforcement
IOC	Interagency operation center
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LNG	Liquefied natural gas
MARAD	U.S. Department of Transportation Maritime Administration
MCAC	Maryland Coordination and Analysis Center
MDA	Maritime Domain Awareness
MEMA	Maryland Emergency Management Agency
MIST	Multimodal Information Sharing Team
MPA	Maryland Port Administration
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NMIO	National Maritime Intelligence Integration Office
NPS	Naval Postgraduate School
OEM	Boston Mayor's Office of Emergency Management
QCHAT	Quality Cargo Handling Action Team
SAR	Suspicious Activity Reporting
USCG	U.S. Coast Guard

Appendix C: Baltimore Systems Guide 2012[2]

Programs & Centers

Anti-Terrorism Advisory Council (ATAC) District of Maryland

In residence in Baltimore, the ATAC is chaired by the U.S. Attorney General and is considered an exemplary counterterrorism effort.

Delmarva Water Transport Committee (DWTC)

http://www.dwtconline.com/

The Delmarva Water Transport Committee (DWTC) is a non-profit organization with headquarters in Salisbury, Maryland. Formed in the fall of 1974, DWTC's mission is to encourage the continuation and further development of waterborne commerce on the rivers, bays and harbors of the Delmarva Peninsula through the promotion of adequate dredging, safe navigation and maintenance and development of harbor and river terminals in such a manner as to protect and conserve the environment.

Maryland Coordination and Analysis Center (MCAC)

The Maryland Coordination and Analysis Center (MCAC), a component of the Maryland State Police and the U.S. attorney's Anti-Terrorism Advisory Council, is the statewide fusion center, established in 2003. The MCAC instituted an all-crimes approach in 2006. The MCAC is a member of the five state/D.C. NCR Fusion Center Directors Exchange Program, which includes analyst exchanges, regional Suspicious Activity Reporting exchanges, Terrorist Screening Center notifications, and exchanges of criminal or border crime data.

Interagency Operations Center (IOC)

The Security and Accountability for Every Port (SAFE Port) Act of 2006 mandated the Department of Homeland Security (DHS) establish Interagency Operations Centers (IOCs) for security in key ports. In response, the Coast Guard began the IOC acquisition project to improve multi-agency maritime security operations and enhance cooperation among partner agencies at 35 U.S. ports. IOCs help port agencies collaborate in the conduct of first response, law enforcement and homeland security operations. Planning for the Baltimore IOC is currently underway.

Joint Harbor Operations Center (JHOC)

Originally planned as a physical facility, planning is now underway for a "virtual" Joint Harbor Operations Center (JHOC) for the Port of Baltimore community. Critical stakeholders are meeting to give input on design and function of the JHOC.

Joint Terrorism Task Force (JTTF)

The Baltimore-based Maryland Joint Terrorism Task Force (JTTF) is responsible for receiving, analyzing, gathering and sharing threat-related information for the state (except for the suburbs of D.C., which fall under the Washington JTTF, part of the FBI's Washington field office.)

---

[2] Sources:
http://projects.washingtonpost.com/top-secret-america/states/maryland/
http://www.uscg.mil/acquisition/ioc/
http://coastguard.dodlive.mil/2011/07/protecting-america-from-threats-delivered-by-sea/
http://www.uscg.mil/acquisition/newsroom/pdf/cg9newslettermar11.pdf
http://www.gao.gov/assets/590/588476.pdf
http://www.gohs.maryland.gov/pdfs/MarlyandMaritimeStrategicSecurityPlan.pdf

Maritime Tactical Operations Group (MTOG)

Started in the spring of 2005, as a Sub-Committee to the USCG Sector Baltimore Area Maritime Security Committee (AMSC), the Maritime Tactical Operations Group (MTOG) is comprised of federal, state and local agencies all working together in a task force style operation. Dedicated members are focused on standardized training, operational procedures, and equipment that would help prevent or respond to any potential maritime terrorist event.

Maryland Maritime Security Team (MMST)

Maryland Maritime Security Team (MMST) is charged by the Governor to work directly with the Maryland Department of Transportation for the development of the Maryland Maritime Strategic Security Plan. The current Maryland Maritime Strategic Security Plan addresses high-level issues, including capabilities, goals, partnerships and jurisdiction. The MMST held monthly group meetings, in addition to focus group meetings, in which Maryland maritime stakeholders, both public and private, were invited to help draft and give feedback on sections of the Plan.

Maryland Joint Operations Center (MJOC)

The Maryland Joint Operations Center (MJOC) is and interagency effort housed in the Maryland Emergency Management Agency (MEMA). Operated round-the-clock by National Guard and emergency management professionals, the MJOC was the first joint civilian-military watch center in the country. In addition to serving as a communications hub for emergency responders statewide and to support local emergency management, the MJOC monitors local, state, national and international events, and alerts decision-makers in Maryland when a situation warrants.

Council of Supply Chain Management Professionals-Baltimore Roundtable

http://baltimorecscmp.org/

CSCMP is and international supply chain and logistics organization dedicated to education. CSCMP is the leading supply chain management professional organization that develops, advances and disseminates supply chain knowledge and research. The Baltimore Roundtable is a volunteer organization that provides educational resources, informational dinner programs, facility tours and valuable networking opportunities to supply chain professionals in the Baltimore area.

Working groups

Area Maritime Security Committee (AMSC) Baltimore/NCR/Hampton Roads

Part of a national USCG effort, the AMSCs are composed of government agencies, commercial industries, and individuals interested in preserving and enhancing the security of our shared waterfront infrastructure and the Marine Transportation System (MTS). The Committees have been created to build an awareness of our maritime activities, identify risks, enhance security activities, improve communications, and to coordinate a rapid response to increased security threat levels. The Committees create, maintain, and exercise federal Area Maritime Security Plans, aimed at minimizing risk during times of heightened threats. These plans will outline scalable activities to be conducted by MTS stakeholders and government agencies to ensure proper precautions are taken to ensure the continued safety and security of our region's infrastructure and MTS.

Federal Agency Quality Working Group (FAQWG)

The Federal Agency Quality Working Group (FAQWG) meets monthly in the Pilots' Association building in downtown Baltimore. Members include the USCG, USDA, Fish & Wildlife Service (FWS), Maritime Exchange, CBP, and several private sector representatives among others.

Port of Baltimore Harbor Safety and Coordination Committee

http://www.mpasafepassage.org/harbor.html

The Harbor Safety and Coordination Committee coordinates interagency actions and activities on issues related to navigation, safety and logistics. The group meets quarterly, in March, June, September, and December and is staffed by the Maryland Port Administration. The Harbor Safety and Coordination Committee took shape in the 1980s, when the Port of Baltimore was improving its navigation system to accommodate the larger cargo vessels. The Maryland Port Administration recognized that the success of these projects would depend on the cooperative efforts of several agencies and organized a committee with representatives from the Maryland Department of Transportation/Maryland Port Administration, U. S. Army Corps of Engineers (Baltimore District and Philadelphia District), United States Coast Guard, and the Association of Maryland Pilots. By 2001, participants also included the National Oceanographic and Atmospheric Administration, Baltimore Maritime Exchange, Maryland Transportation Authority, Maryland Department of Natural Resources Police, tugboat operators, dredging companies, and other state agencies responsible for water safety and security.

Quality Cargo Handling Action Team (QCHAT)

The Quality Cargo Handling Action Team (QCHAT) initiative was created as a vehicle to assess performance areas, identify problems, and take corrective action steps to improve the quality handling of the cargo at the Port of Baltimore (POB). QCHAT is a collaborative team approach to prevent any type of damage to customer's cargo. The vision of the QCHAT initiative is to "set the standard for global quality and excellence in cargo handling at Maryland's Port of Baltimore." Additionally the QCHAT measures quality factors to prevent problems from occurring. Specifically, the QCHAT currently focuses on three categories of cargo: 1) Autos (specifically), 2) Ro/Ro (generally) and 3) Containers. The QCHAT membership is representative of the wider Port of Baltimore community which includes the steamship lines, manufacturers, stevedores, processors, terminal operators, Steamship Trade Association (STA), Maryland Port Administration (MPA), the International Longshoremen's Association (ILA), and the Maryland Transportation Authority Police (MdTAP), and other key partners in the POB.

Information Systems

ASIS Toolkit

http://www.asisonline.org/toolkit/toolkit.xml

ASIS International is an organization for security professionals. Founded in 1955, ASIS develops educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. It also publishes Security Management magazine. The ASIS Security Toolkit available online provides a variety of links, information and guidance from security experts.

DHS Daily Open Source Infrastructure Report

http://www.dhs.gov/dhs-daily-open-source-infrastructure-report

The DHS Daily Open Source Infrastructure Report is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan.

Delmarva Water Transport Committee (DWTC)

http://www.dwtconline.com/

The Delmarva water transport Committee (DWTC) is a non-profit organization with headquarters in Salisbury, Maryland. Formed in the fall of 1974 by a small group of people who were concerned about the future of waterborne commerce on the Delmarva Peninsula. Their mission is to encourage the continuation and further development of waterborne commerce on the rivers, bays and harbors of the Delmarva Peninsula through the promotion of adequate dredging, safe navigation and maintenance and development of harbor and river terminals in such a manner as to protect and conserve the environment.

"If you see something, say something"™ (DHS)

http://www.dhs.gov/if-you-see-something-say-something-campaign

In July 2010, the Department of Homeland Security (DHS), launched a national "If You See Some-thing, Say Something™" campaign –to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities. The "If You See Something, Say Something™" campaign - originally implemented by New York City's Metropolitan Transportation Authority. DHS launched the "If You See Something, Say Something™" campaign in conjunction with the Department of Justice's Nationwide Suspicious Activity Reporting (SAR) Initiative - an administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and ensure the sharing of those reports with the FBI-led Joint Terrorism Task Forces for further investigation and fusion centers for analysis.

Homeland Security Information Network (HSIN)

Maryland was one of six states (through the NCR) to initially test the DHS Homeland Security In-formation System-Intel (HSIN-Intel) pilot, which allows fusion centers to directly share classified information to identify trends and patterns that may represent links to terrorism.

Homeport (USCG)

https://homeport.uscg.mil/

Launched by the U.S. Coast Guard (USCG) in October 2005, Homeport is the official Coast Guard information technology system for maritime security, created to provide information and services to the maritime community and the public over the Internet. The system was intended to serve as the primary means for the day-to-day management and communication of port security matters with Area Maritime Security Committee members, commercial vessel and facility owners and operators, government partners, and the public. A publicly accessible internet portal, Homeport provides access to information necessary to support increased information sharing requirements among Federal, state, local and industry decision makers for security management and increased maritime domain awareness. Homeport also serves as the Coast Guard's communication tool designed to support the sharing, collection and dissemination of sensitive but unclassified information to targeted groups of registered users within the port community.

Intelligent Closed Circuit Television (iCCTV)

The major local, state, and federal stakeholders in Maryland's maritime domain participate in the Maryland's statewide Intelligent Closed Circuit Television (ICCTV) program. The ICCTV program is an advanced system for sharing multiple formats of video and other imagery from multiple sources with operations centers, responders and as appropriate, the public. Ongoing enhancements to ICCTV include more sharing with private sector partners and increased bandwidth and bi-directional mobile (land, air, and sea) imagery.

iJET Daily Intelligence Briefing

http://www.ijet.com/index.aspx

iJET is an intelligence-driven provider of operational risk management solutions, working with more than 500 multinational corporations and government organizations. iJET capitalizes on proprietary technology and a network of security, intelligence and geopolitical experts to deliver a full array of customized intelligence, preparedness and response solutions. Our solutions allowing decision-makers and organizations to anticipate, respond to and mitigate from business disruptions. The iJET Daily Intelligence Briefing is a concise report flagging noteworthy risk-related events and developments around the world.

InfraGard Maryland Members Alliance (IMMA)

http://www.infragard.net/chapters/baltimore/

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.. InfraGard Maryland Members Alliance (IMMA), the Maryland Chapter of InfraGard, is headquartered in the FBI's Baltimore Field Office. Now with over 880 registered members, and with meetings and events held at select venues throughout the state each year, the IMMA has grown into one of the most active InfraGard Chapters in the nation.

Maritime Law Enforcement Information Network (MLEIN)

The Maryland Law Enforcement Information Network (MLEIN) allows agencies and groups across the state to share information on a real-time basis. Hosted by the Maryland Natural Resources Police, MLEIN is a data-sharing system which establishes a communication network of voice, video and data that permits command level personnel to work in concert toward a satisfactory resolution of a marine event. It represents a partnership of governmental agencies (both regional and federal), first responders, NGOs and the private sector to increase the efficacy of maritime response. Depending on need, each group may be able to access views from cameras and other recording devices across the state, as well as to establish virtual command centers across a large geographic area. MLEIN will be rolled out to stakeholders on December 31, 2012.

The Overseas Security Advisory Council (OSAC) website

https://www.osac.gov/Pages/Home.aspx

The Overseas Security Advisory Council (OSAC) was created in 1985 under the Federal Advisory Committee Act to promote security cooperation between American private sector interests world-wide and the U.S. Department of State. The OSAC "Council" is comprised of 30 private sector and four public sector member organizations that represent specific industries or agencies operating abroad. The Council provides direction and guidance to develop programs to support the U.S. private sector overseas. The Department of State's Bureau of Diplomatic Security (DS) implemented the following recommendations for OSAC: to create the OSAC website, to create a Country Council Program, and to develop a Research and Information Support Center (RISC). A primary goal of OSAC is to develop an effective security communication network. The OSAC Daily News page of their website posts global items of interest in a quickly accessible digest format at https://www.osac.gov/Pages/News.aspx

WatchKeeper (USCG)

The Interagency Operations Center (IOC) information management system, WatchKeeper coordinates and organizes port security information to help the Coast Guard and its port partners make the best use of their resources to keep America's ports safe.

Informal Communications

Port of Baltimore stakeholders use several informal communications channels to pass security related all-hazards information including:

- Telephone
- Face-to-face conversations
- Instant messaging
- Email
- Event-driven threat and security briefs

Private Sector Organizations

Association of Maryland Pilots

http://www.marylandpilots.com/

Founded in 1852, The Association of Maryland Pilots is the oldest state codified organization of Pilots in the nation. The Maryland Pilots have always been known for accomplishing "first's." They continue to be a progressive leader in the world of piloting by being strong advocates of technology, training, and accountability.

Baltimore Maritime Exchange (BME)

http://www.balmx.org/default.aspx

The Baltimore Maritime Exchange (BME) has been providing access to live real time vessel reporting 24/7 to members via their secure website since September of 2002. Working cooperatively with federal, state and local agencies, steamship agents, terminal operators, pilots, tug companies, stevedores, and numerous service providers, the BME tracks, identifies, logs, and provides accurate and timely information on vessel activity in the Port of Baltimore. This information includes a traditional arrival/departure report, a three day due in list, weekly tentative arrivals report, and monthly Traffic/Flag Summary Reports.

Baltimore Port Alliance (BPA)

http://www.baltimoreportalliance.org/

The BPA is a non-profit group of maritime business representatives dedicated to addressing the needs and interests of businesses and individuals who make their living and support their families through maritime commerce. BPA efforts are focused on: 1) maintaining and improving maritime commerce, 2) monitoring legislation that affects the safety and health of the Port and its navigational channels in the Chesapeake Bay, 3) adhering to federal and state maritime/seaport security policies, and 4) protecting industrial/commercially zoned property surrounding the Port of Baltimore waterfront community.

Chesapeake Energy Services

http://www.cestugs.com/

Conceived in 2003, Chesapeake Energy Services, LLC ("CES") addresses service, safety and security concerns in providing fully integrated ship assistance and logistics support to liquefied natural gas (LNG) carriers serving the Dominion Cove Point LNG terminal, the nation's largest LNG import facility. CES leverages the collective experience, process improvements, and best practices of its operating companies and partners to support responsible stewardship of the marine environment.

CSX Railroad

http://www.csx.com/

CSX is a leading supplier of rail-based freight transportation in North America. More information about CSX is available on their website.

Dominion Cove Point LNG

https://www.dom.com/business/gas-transmission/cove-point/index.jsp

Dominion Cove Point LNG is located on the Chesapeake Bay in Lusby, Maryland, south of Balti-more. It is one of the nation's largest liquefied natural gas (LNG) import facilities. Dominion Cove Point will play an increasingly critical role in coming years given that demand for natural gas is ex-pected to grow through the next decade.

Maryland Motor Truck Association (MMTA)

http://www.mmtanet.com/

The Maryland Motor Truck Association (MMTA) is a non-profit, member-driven trade organization that has been serving Maryland's commercial trucking industry since 1935. Today, MMTA is one of the largest trucking associations in the country, representing 1,000 member companies.

Potomac River Rescue Association (PRRA)

The Potomac River Rescue Association (PRRA) serves the people of Virginia, Maryland and Washington DC along the Upper Potomac River, coordinating local law enforcement, fire & rescue, USCG, state and federal agencies and Towing & Salvage companies. PRRA members provide for a quick and coordinated response through water and land rescues, using the shared resources of the member groups.

Potomac Riverboat Company

http://potomacriverboatco.com/

Potomac Riverboat Company is a private company that began as Potomac Boat Tours in 1974. Potomac Riverboat Company's vessels and services are based in the colonial seaport of Alexandria, Virginia, just 8 miles south of Washington, D.C.

City Agencies

Mayor's Office of Emergency Management (MOEM)

http://emergency.baltimorecity.gov/

The mission of the Baltimore City Mayor's Office of Emergency Management (MOEM) is to maintain the highest level of preparedness to protect Baltimore's citizens, workers, visitors, and environment from the impact of natural and man-made disasters. To achieve this mission, MOEM will implement a comprehensive program of disaster mitigation, preparedness, response, and recovery. On a day-to-day basis, MOEM's primary function is to implement programs that prepare the City for major emergencies. MOEM is responsible for citywide, interagency preparedness. MOEM ensures that the City's overall emergency plans integrate the procedures and resources of all City agencies and outside organizations. MOEM serves as the link between the City and other entities – regional, State, Federal, non-profit, and private sector partners – for emergency planning and operations.

Baltimore Fire Department

http://www.baltimorecity.gov/Government/AgenciesDepartments/Fire.aspx

The Baltimore City Fire Department serves a geographic area of 81 square miles and a population of more than 640,000 residents. The department has over 1800 members who are divided into two management branches – Emergency Operations and Planning and Administration. The department responds to more than 235,000 emergency 911 calls per year.

Baltimore Police Department (BPD)

http://www.baltimorepolice.org/

The Baltimore Police Department (BPD) is the 8th largest municipal police force in the United States, staffed by nearly 4,000 civilian and sworn personnel. The department's jurisdiction covers Maryland's largest city, with a population of 641,000.

State & Regional Agencies

Baltimore County Fire Department

http://www.baltimorecountymd.gov/Agencies/fire/index.html

The Baltimore County Fire Department provides fire protection, emergency medical and emergency rescue to the county's more than 800,000 citizens. The Fire Department serves a diverse area, including heavy industrial areas, small towns, suburban neighborhoods and farmland. The northern two-thirds of the county is almost exclusively rural, with denser suburban populations and industrial areas located, east to west, in a horseshoe surrounding Baltimore City.

Baltimore County Police Department (BCoPD)

http://www.baltimorecountymd.gov/Agencies/police/index.html

The Baltimore County Police Department enforces the laws and ordinances of the state and county, safeguards life and property, prevents and detects crime, preserves the peace, and protects the rights of all citizens.

Calvert County Sheriff's Office

http://www.co.cal.md.us/residents/safety/law/sheriff/

The Calvert County Sheriff's Office was established in 1654 and is the primary law enforcement agency for the county.

Charles County Sheriff's Office

http://www.ccso.us/index.php

The Charles County Sheriff's Office is a full-service law enforcement agency responsible for preventing and investigating crime, operating the county detention center and performing the court-related functions of a traditional sheriff's office. The Sheriff's Office has more than 600 sworn, corrections and civilian employees, and is accredited by the Commission on the Accreditation of Law Enforcement Agencies.

Delaware Valley Intelligence Center (DVIC)

Maryland is a participant in the Philadelphia-based Delaware Valley Intelligence Center (DVIC), a four-state (Pennsylvania, Delaware, Maryland, New Jersey), 12-county initiative.

Governor's Office of Crime Control and Prevention (GOCCP)

The GOCCP serves as a broad resource to improve public safety. It educates, connects, and empowers Maryland's citizens and public safety entities through innovative funding, strategic planning, crime data analysis, best practices research and results-oriented customer service. Contact: http://www.goccp.maryland.gov

Governor's Joint Executive Committee for Homeland Security (JEC)

The JEC is a group of Senior Officials from various inter-related disciplines within State Govern-ment designed to advise the Governor on matters of Homeland Security. This group focuses on the Governor's 12 Core Goals for Homeland Security, the application of the principles, the progress of the deliverables, and the measure of the programs and projects successes. The group also focuses on

related Federal Grant funding and Federal Congressional Earmarks to accomplish these Core Goals. The group is chaired by the Governor's Homeland Security Advisor.

Harford County Sheriffs Office

http://www.harfordsheriff.org/

The Harford County Sheriff's Office provides professional police, courts and correctional services to the citizens of Harford County. Having as its motto, Courage, Honor, and Integrity in the Pursuit of Justice, the Sheriff's Office has become an integral working part of the community, providing for the safety, health and well being of county residents.

Prince George's County Police Department

http://www.princegeorgescountymd.gov/government/publicsafety/police/

As the 29th largest police agency in the nation, the Prince George's County Police Department (PGCoPD) serves approximately 800,000 citizens throughout the County. In 2001, the Department answered close to 500,000 calls for service. This department currently has an authorized strength of 1,420 officers and 263 civilians.

Maryland Department of Public Safety and Correctional Services (DPSCS)

The Maryland Department of Public Safety and Correctional Services (DPSCS) is the statewide law enforcement agency.

Maryland State Police (MSP)

The Maryland State Police (MSP) in Pikesville addresses foreign and domestic security threats and includes a Homeland Security and Investigation Bureau. The MSP provide intelligence and other Law Enforcement functions that include but are not limited to interdiction, tactical resources aviation, crime lab and personnel throughout the State of Maryland. The Office of the State Fire Marshal Bomb Squad, a law enforcement agency within the Department of State Police, coordinates bomb squad response. The Maryland State Police shares concurrent jurisdiction with other state and local law enforcement agencies, including the Maryland Natural Resources Police.

Maryland Statistical Analysis Center (MSAC)

The Maryland Statistical Analysis Center (MSAC) is the research, development and evaluation component of the Governor's Office of Crime Control & Prevention (GOCCP).

Maryland Emergency Management Agency (MEMA)

http://mema.maryland.gov/Pages/AboutMEMA.aspx

The Maryland Emergency Management Agency (MEMA), coordinates disaster/emergency preparedness and provides logistical and infrastructure support to the Governor's Office of Homeland Security. While MEMA is under the authority of the Maryland Military Department's adjutant general, during emergencies the governor may assume direct authority over the agency and the executive director of MEMA reports directly to the governor. The MEMA Operations Directorate includes critical-infrastructure protection (CIP). To assist in CIP, a DHS Protective Security Advisor is located in Baltimore.

Maryland Governor's Office of Homeland Security

http://www.gohs.maryland.gov/

The Maryland Governor's Office of Homeland Security is a coordinating office, leading the development of policies, priorities and strategy for homeland security and assisting state and local agencies in the implementation of their counterterrorism and public safety missions.

Maryland Natural Resources Police/Department of Natural Resources (MNRP)

http://www.dnr.state.md.us/nrp/

Throughout Maryland, the NRP serves as the primary search and rescue State agency on Maryland waters and in rural areas of the state. The NRP routinely patrol Maryland waterways and conduct law enforcement patrols related to resource conservation, boating safety, criminal enforcement, search and rescue and homeland security on a round the clock basis.

Maryland Port Administration (MPA)

http://www.mpa.maryland.gov/

As one of the Modes within the Maryland Department of Transportation, the Maryland Port Administration (MPA) is responsible for operating the six public marine terminals located in the Port of Baltimore. The MPA handles all types of cargo to include Containers, Roll-On/Roll-Off cargo, auto exports, break-bulk, and others. The MPA also operates a Cruise Terminal at the South Locust Point Terminal with year-round cruising scheduled for years in advance. Within the MPA, the Office of Security is responsible for coordinating all security functions at the MPA Maritime Regulated Facilities. The Office of Security has contract uniform security guards that are utilized for access control, while the Maryland Transportation Authority Police provide full-time law enforcement services through their Port Detachment. The Office of Security works with the Area Maritime Security Committee, federal authorities, a number of state and local law enforcement agencies, and other Port partners to coordinate security preparedness, response, and situational awareness with the Port community.

Maryland Transportation Authority Police (MdTAP)

http://www.mdta.maryland.gov/Police/policeMain.html

The Maryland Transportation Authority Police (MdTAP) have law enforcement jurisdiction over bridges, tunnels and certain roadways, and for facilities under the management of the Maryland Port Administration, the Maryland Transportation Authority, and the Baltimore Washington International Thurgood Marshall Airport. Consequently, the Maryland Transportation Authority Police has a de facto primary role for a variety of potential maritime incidents.

Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN)

Maryland is a member of the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Working Group (MAGLOCLEN)

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Maryland is a member of Multi-State Information Sharing and Analysis Center (MS-ISAC).

Southern Maryland Information Center (SMIC)

The Southern Maryland Information Center (SMIC), covering Calvert, Charles and St. Mary's counties, was established in 2007 and collects, evaluates and disseminates information on known or suspected criminal violators, groups and organizations.

Washington/Baltimore High Intensity Drug Trafficking Area (HIDTA)

The Washington/Baltimore High Intensity Drug Trafficking Area (HIDTA) in Greenbelt performs criminal intelligence analysis for parts of Maryland, the District of Columbia and, in Virginia, Alexandria city and Loudoun, Prince William, Arlington and Fairfax counties. The HIDTA Watch Center provides tactical and actionable intelligence to law enforcement throughout Maryland, Virginia and D.C.

Western Maryland Information Center (WMIC)

The Western Maryland Information Center (WMIC), located in Frederick and established in 2008, is a second regional data fusion center, composed of law enforcement agencies from Frederick and Washington counties.

Washington Regional Threat Analysis Center (WRTAC)

Maryland also falls under the Washington Regional Threat Analysis Center (WRTAC) in D.C.

Federal Agencies

Customs and Border Protection (CBP)

The United States Custom and Border Protection (CBP) is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. The CBP also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. In the maritime domain, the CBP has priority in cases involving international trade, immigration and drug laws.

Department of Homeland Security (DHS)

http://www.dhs.gov/

The mission of the U.S. Department of Homeland Security (DHS) is to secure the nation from a wide variety of threats. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cyber-security analyst to chemical facility inspector. DHS combined 22 different federal departments and agencies into a unified, integrated cabinet agency when it was established in 2002.

Department of Transportation (DOT)

http://www.dot.gov/

The U.S. Department of Transportation (DOT) was established by an act of Congress on October 15, 1966 – and the agency's first official day of operation was April 1, 1967. The DOT mission is to "serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future."

Federal Emergency Management Agency (FEMA)

http://www.fema.gov/

The Federal Emergency Management Agency (FEMA) coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. FEMA can trace its beginnings to the Congressional Act of 1803. As of October 8, 2011, FEMA has 7,474 employees across the country – at Headquarters, the ten regional offices, the National Emergency Training Center, Center for Domestic Preparedness/Noble Training Center and other locations.

Federal Bureau of Investigation (FBI)

http://www.fbi.gov/

As an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. As of September 2012, the FBI had a total of 36,074 employees – including 13,913 special agents and 22,161 support professionals, such as intelligence analysts, language specialists, scientists, information technology specialists, and other professionals. The FBI's Baltimore field office operates resident agencies and satellite offices in Annapolis, Bel Air, Calverton, Frederick and Salisbury.

Immigration and Customs Enforcement (ICE)

http://www.ice.gov/

U.S. Immigration and Customs Enforcement (ICE) is the principal investigative arm of the U.S. Department of Homeland Security (DHS) and the second largest investigative agency in the federal

government. Created in 2003 through a merger of the investigative and interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service, ICE now has more than 20,000 employees in offices in all 50 states and 47 foreign countries.

Information Sharing Environment (ISE)

http://ise.gov/

The Information Sharing Environment (ISE) provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security.

U.S. Coast Guard (USCG)

http://www.uscg.mil/

The U.S. Coast Guard (USCG) is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. Since 1790 the Coast Guard has safeguarded our Nation's maritime interests and environment around the world. The Coast Guard is an adaptable, responsive military force of maritime professionals whose broad legal authorities, capable assets, geographic diversity and expansive partnerships provide a persistent presence along our rivers, in the ports, littoral regions and on the high seas. In 2011, the USCG included over 43,000 active duty members, over 7,800 reservists, over 8,300 civilian employees, and almost 33,000 volunteer Auxiliarists.

National Maritime Intelligence Intelligence-Integration Office (NMIO)

http://www.nmic.gov/

Formerly the National Maritime Intelligence Center, the National Maritime Intelligence-Integration Office (NMIO) is the unified maritime voice of the U.S. Intelligence Community (IC). It operates as an IC Service of Common Concern to integrate and streamline intelligence support, providing a whole of government solution to maritime information sharing challenges. NMIO neither collects nor produces intelligence. It breaks down barriers to information sharing and creates enabling structures and cultures to set the conditions for maritime partners to optimally share data. NMIO works at the national and international level to facilitate the integration of maritime information and intelligence collection and analysis in support of national policy and decision makers, Maritime Domain Awareness (MDA) objectives, and interagency operations, at all levels of the U.S. Government (USG).text

FBI Field Intelligence Group (FIG)

The Federal Bureau of Investigation (FBI) operates a Field Intelligence Group (FIG) in Baltimore responsible for all parts of Maryland except the National Capital Region, which falls under the FBI's Washington field office.

ICE Field Intelligence Group (FIG)

The Immigration and Customs Enforcement (ICE) Field Intelligence Group in Baltimore has jurisdiction over the Baltimore area and those parts of Maryland that are not part of the National Capital Region.

LIST OF REFERENCES

1 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. Last accessed 29 January 2010 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-LongBeach%202008.pdf

2 Salem, Anita, Wendy Walsh and Lyla Englehorn (2009). "Industry and Public Sector Cooperation for Information Sharing: Ports of the Puget Sound," a publication of the Naval Postgraduate School. July 2009. Last accessed 9 November 2012 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Puget%20Pound%202009.pdf

3 Salem, Anita, Susan Hocevar, Wendy Walsh and Lyla Englehorn (2010). "Industry and Public Sector Cooperation for Information Sharing: Ports of Delaware Bay," a publication of the Naval Postgraduate School. December 2010. Last accessed 9 November 2012 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Delaware%20Bay%202010.pdf

4 Salem, Anita, Wendy Walsh and Lyla Englehorn (2010). "Industry and Public Sector Cooperation for Information Sharing: Port of Honolulu," a publication of the Naval Postgraduate School. Spring 2010. Last accessed 9 November 2012 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Honolulu%202010.pdf

5 Salem, Anita, Hocevar, S.P., Wendy Walsh and Lyla Englehorn (2011). "Industry and Public Sector Cooperation for Information Sharing: Port of Boston," a publication of the Naval Postgraduate School. Fall 2011. Last accessed 9 November 2012 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Boston%202011.pdf

6 Hocevar, S.P., Thomas, G.F. and Jansen, E. (2006) "Building Collaborative Capacity: An Innovative Strategy for Homeland Security Preparedness," in Advances in Interdisciplinary Studies of Work Teams: Innovation Through Collaboration, Vol. 12:255-74, M.M. Beyerlein, S.T. Beyerlein, and D. A. Kennedy, eds. Oxford: Elsevier JAI Press.

7 Hocevar, S.P., Jansen, E. and Thomas, G.F. Inter-Organizational Collaboration: Assessing the Challenge. Homeland Security Affairs Journal, Vol 7, The 9/11 Essays (September, 2011). www.hsaj.org.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943

4. Susan Page Hocevar, PhD
   GSBPP
   Naval Postgraduate School
   Monterey, CA 9394

5. Wendy Walsh
   MOVES
   Naval Postgraduate School
   Monterey, CA 93943

6. Kenneth Holliday
   Office of the Program Manager, Information Sharing Environment
   ISE Mission Programs Division
   2100 K Street, NW
   Suite 4000
   Washington, DC 20511