MIST

Multimodal Information Sharing Team

Oakland Seaport, CA

Industry and Public Sector Cooperation for Information Sharing

Wendy Walsh
Anita Salem
Lyla Englehorn
Susan Page Hocevar

Table of Contents

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. After conducting four MIST workshops, the interconnection of the maritime domain to other modalities in terms of information sharing became a natural expansion of the research. Beginning in Boston, the MIST framework and process for the collaborative exploration of information sharing embraced the larger port multimodal community. The MIST continues to emphasize the private sector perspective to ensure that government stakeholders are leveraging these critical players in the sharing of all hazards threat information protecting our global supply chain.

To date, MIST has held seven events throughout the U.S. at the ports of Los Angeles/Long Beach, the Puget Sound, Honolulu, the Delaware Bay, Boston, Baltimore and most recently Oakland. As highlighted in our five minute video report[1], a consolidated view of our research shows that while the commodities and geography vary from port to port, the people and issues are more alike than different when it comes to sharing information. Our earlier findings of individual ports show that information sharing between industry and government is enhanced by improving collaboration, increasing cultural awareness, improving communication tools, and aligning financial and non-monetary incentives with industry motivations. [2,3,4,5,6]

The action planning focused on strengthening local collaboration and improving local information sharing networks

As we began to research and understand the Port of Oakland, we quickly found that while there is some overlap between the air and maritime information sharing communities, the domains would best be served by two separate MIST workshops. This would allow us to facilitate the workshop at a meaningful depth to capture valued practices as well as formulate action items to improve information sharing. It was determined that the Maritime MIST workshop would occur first and the Air MIST workshop would occur later this summer.

Working with the strong leadership of the Port of Oakland, we pulled together a steering committee meeting for the Maritime MIST workshop. This steering committee was unique from prior MIST efforts as we had a very strong voice from the trucking community. We also had our more typical support from maritime shipping industry, DHS Protective Security Advisors, US Coast Guard (USCG), the Marine Exchange, the Department of Transportation Maritime Administration (DOT-MARAD) and the Northern California Regional Intelligence Center (NCRIC).

The location of this MIST workshop was the Oakland Maritime Support Services (OMSS) space. OMSS is a clearinghouse organization supporting the trucking industry serving the Port of Oakland. OMSS was a very gracious host and this location facilitated the rest of the community learning more about the trucking industry presence and efforts in Oakland. Many of the participants had never been to this location prior to the workshop.

During the day and a half workshop, we explored multimodal issues facing the maritime community in Oakland and led the participants through a process of action planning. The action planning focused on strengthening local collaboration and improving local information sharing networks. In addition, participants looked at issues related to cybersecurity.

Using the Inter-Organizational Collaborative Capacity (ICC) model[7] developed by one of our researchers, we encouraged the participants to explore how their networks could be improved. Collaborative capacity is the ability of an organization(s) to enter into, develop, and sustain inter-organizational systems in pursuit of collective outcomes. As shown in Figure 1, there are a number of factors that impact a system's ability to collaborate. Organizations have their own missions with goals and incentives that sometimes conflict with one another; agencies often have histories of distrust that are hard to alter; leaders may not actively support collaborative efforts; and coordination systems and structures that might support collaboration are often lacking.[8] Using the ICC model, MIST investigated the collaborative capacity of the Oakland community along five dimensions: purpose, structure, mechanisms, incentives, and people. The first domain, purpose, explores the underlying strategic factors impacting collaboration, such as felt need, leadership actions, and resources. The second domain, structure, probes the system's support structures, for example interagency task forces and flexible processes. Mechanisms, the third domain, refer to the technical tools and social processes that are utilized to support collaboration. The fourth domain, incentives, relates to organizational reward systems. And finally, the people dimension explores the personal aspects of collaboration, including trust and personal competencies.

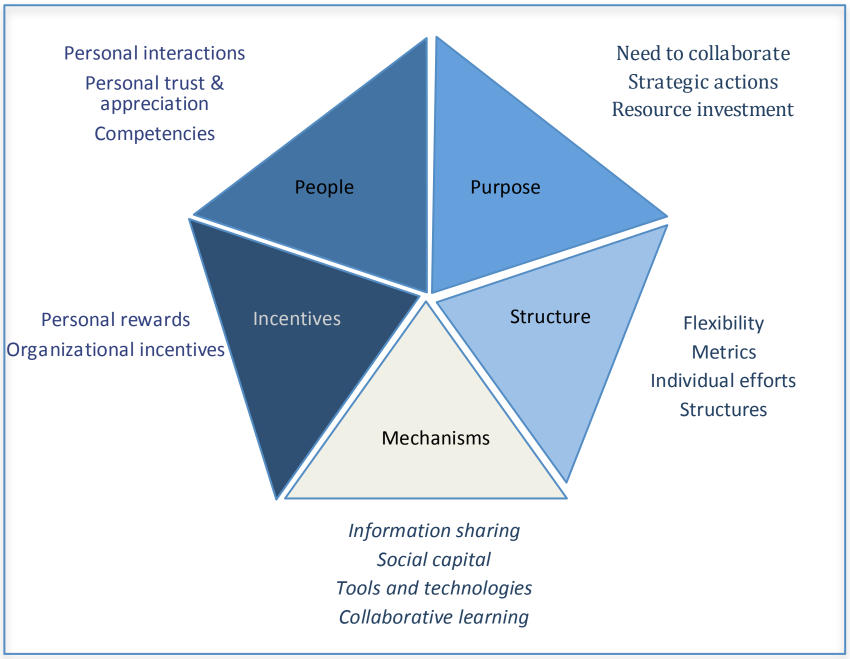


Figure 1: Collaborative capacity

Spotlight: OT-511

The Oakland Truckers Traffic Information System (OT-511) is a real-time alert system that uses a cell phone's texting feature to inform truckers of traffic congestion at specific locations throughout the port of Oakland.

Background

The Metropolitan Transportation Commission (MTC) and the West State Alliance (WSA) are partners in offering a free information service to Bay Area truckers. This service informs truckers of real time traffic congestion in the area. The system has three main elements: a Twitter feed, access to 511, and outreach by the Metropolitan Transportation Commission (MTC) and the West State Alliance (WSA.)

Twitter feed

Twitter is a service that allows a user to post short messages on the web or by phone and have them delivered to multiple recipients. It is a "push" delivery system where users automatically receive information. Users can follow the OT-511 service by sending a text message ('Fast Follow'), by creating a Twitter account via phone, or by creating a Twitter account via the web. The simplest option is the 'Fast Follow' because it is free and does not require a Twitter account, username, or email address-which many truckers do not have.

511 linkage

The 511 Traveler Information Program is a phone and web source for Bay Area traffic, transit, rideshare, and bicycling information. The service is free and available on demand by phone or web 24 hours a day. It is a primarily a "pull" system, where users must reach out for the information. 511 also offers a customized service called My-511 that can provide travel time alerts for saved trips. This requires the creation of an online account.

Outreach efforts

Both MTC and WSA are engaged in developing and delivering training and promotional materials for the OT-511 system. WSA is a trade association that represents the interests of independent trucking companies when working with steamship and stevedoring companies operating in West Coast ports. The MTC is the transportation planning, coordinating and financing agency for the nine-county San Francisco Bay Area.

Implementation

OT-511 is a combination system that includes twitter broadcast feeds, 511 information, and outreach. It is one way only—truckers cannot at this point send information directly to the Twitter feed. The sponsors of OT-511 have developed a special twitter account for the Oakland Truckers that uses the 'Fast Follow" Twitter-to-text option. This is the heart of the OT-511 system. This Twitter feed will consolidate information by re-tweeting 511 Twitter information and creating global 'My 511' trips that are appropriate for the majority of the Bay Area (101 from Gilroy to Cloverdale, Hwy 80 from San Francisco to Fairfield, Hwy 580 from San Rafael to Tracy, Hwy 17 from San Jose to Santa Cruz, etc.) OT-511 is currently focused on increasing enrollment and awareness within the trucking community. Truckers have disparate skills and knowledge of technology and social media and even with the simplified Twitter approach the technology barriers are limiting participation.

Impact

The goal of OT-511 is to improve communication with the trucking community in order to reduce congestion on highways, reduce greenhouse gas emissions, and facilitate efficient supply chain operations. The success of the program will be measured by the number of active users and the amount of greenhouse gas reductions. This system is in the early stages of adoption and may be suitable for providing real-time security information to a key port community. During the workshop, stakeholders from the trucking industry identified the OT-511 network as a possible method for disseminating regional security alerts.

Findings

Using both large group discussions and small group activities, the workshop focused on learning more about local information sharing partners, evaluating the local methods used for sharing all-hazards threat information, and exploring the issue of cyber-security.

Information Sharing Partners

To explore the question of *who* needs to share, a large list of organizations was provided on a poster to the group. This list is summarized in the Appendix. The list was divided up into six information sharing mechanisms: formal information systems, informal information systems, private sector stakeholders, public agency stakeholders, programs and centers, and working groups. The group was asked to look at the list and add any entities that might be missing. This resulted in a list of 102 possible nodes for information sharing in the Port of Oakland.

The group was then introduced to the concept of weak and strong ties. This concept, while most cited in the field of sociology as introduced by Mark Granovetter[9], has been applied across many domains as referenced in more popular books of late*, The Tipping Point*[10] and *Linked*[11]. Granovetter provides four ways to assess the strength of a tie:

- The amount of time spent with the other
- The intensity of experience together
- The intimacy or personal awareness we have about each other
- The exchanging of assistance or favors.

The more our relationships embody these elements the stronger the tie.

For the workshop, we had participants indicate their strong and weak ties on the large poster. Participants representing public sector stakeholders were provided with different colored markers than industry in order to evaluate any differences. This exercise was conducted to expand the thinking of the relationships between stakeholders in terms of information sharing and also to help the MIST team better understand the nature of the linkages.

By identifying strong ties, weak ties, and discussing the relative impacts of these relationships, we see the different ways that government and industry partners build relationships. Strong ties are important as they depict relationships with deeper impact. Within the six types of mechanisms, government and private sector participants aligned in how they ranked their strong ties in only two categories—informal information systems and public stakeholders. Both private sector and government stakeholders reported strong ties with the US Coast Guard (USCG) and US Customs and Border Protection (CBP). Public Sector participants also included the San Francisco Police Department (SFPD) as one of the strongest public sector ties. It's not surprising that private sector

Both private sector and government stakeholders agreed that the USCG and CBP were the strongest public sector stakeholders

participants ranked USCG, CBP, and SFPD as strong ties as they all serve in a regulatory role for industry stakeholders. However, the public sector also rated the Northern California Regional Intelligence Center (NCRIC) as a strong tie. The NCRIC is a fusion center that is primarily used by government agencies and is now beginning to reach out locally to the maritime industry (see sidebar). Both public and private sectors agreed that email was the most important system for sharing threat information.

Strong ties are not necessarily superior to weak ties. A weak tie can connect communities that don't necessarily engage regularly. Weak ties often develop in more organic ways than more formal relationships such as with a regulatory body and therefore can be a critical node to connect people, programs, working groups or systems. For weak ties, the contrast between the public sector and industry continued with only one common top ranking weak tie in the category of programs and centers—the Joint Terrorism Task Force (JTTF.) The most frequently mentioned weak tie for industry stakeholders in the category of public sector organizations, was the Federal Bureau of Investigation (FBI). The public sectors' most ranked weak tie was Homeport from the category of formal information sharing systems.

In prior workshops we have completed this exercise without ranking the weak and strong ties. Adding this element allows us to understand the information-sharing network of this port to a greater depth by providing a sense of how strong the relationships are. In continuing to collect this ranked data we will be able to surface trends from port to port as well as possibly map information sharing capabilities across ports.

Spotlight: Northern California Regional Intelligence Center

The Northern California Region Intelligence Center (NCRIC) is one of seventy-eight fusion centers that make up the National Fusion Center Enterprise. Fusion centers are intended to serve as a focal point to collect, analyze, synthesize and share threat related information between federal, state, local and private sector partners. They provide intelligence products to partners as well as provide training and connection to other stakeholders.

Implementation

Partnering with the NCRIC is achieved through membership. There are three primary types of membership: Law Enforcement Agency, Public Safety/Government, and Private Sector. Private Sector partner members must meet the following criteria:

- Own or work for a designated critical infrastructure of key resource asset
- Have a management, supervisorial and/or analytical role in the areas of personal, physical or technological security, emergency management, business continuity and/or resiliency.
- They must also be able to pass a background review to confirm the first two criteria as well as address any criminal history
- All members are required to be citizens or a legal permanent resident of the United State of America.
- Once vetted the applicant must complete a nondisclosure agreement describing the appropriate handling of sensitive or controlled information.

The NCRIC currently provides a number of information products to their members. These products include a reports of suspicious activity, real time information on incidents, vulnerability assessments, threat assessments, and summaries and analysis of cyber, terrorism, and Gang threats. The "Partner Update Brief" is released twice weekly and includes suspicious activity reports. These reports provide ranked descriptions of suspicious activities, brief descriptions of regional crime events, and recent alerts (with analysis.)

Impact

The NCRIC is a critical information-sharing node in this region and has the capacity to expand the threat and security information flow of the multimodal security community. The private sector outreach officer has been very active in the MIST planning and workshops demonstrating the strong value this organization has on developing private sector partnerships to improve information sharing. For more information on the NCRIC visit their website at https://ncric.org.

Local Information Sharing

To better understand the collaborative capacity of Oakland information sharing, participants divided into three groups. These groups used a Force Field Analysis approach to examine all-hazards information sharing. This involved envisioning a desired future state for information sharing, describing the relevant current state characteristics, and then identifying barriers and enablers to moving from current to desired future state. Participants then identified specific recommended improvements for these systems. Each group focused on different mechanisms that had been identified in preliminary site interviews:

1. Existing multipurpose networks
2. Future Oakland Domain Awareness Center (DAC)
3. Cybersecurity

As a result, in the first two of these break out sessions, participants identified key mechanisms for sharing and discussed how they could be leveraged to improve local sharing of threat information. The third topic of cybersecurity, which was a new topic for MIST, revealed that more discussion and additional participants representing the information technology sector would need to be included to adequately understand the information sharing needs of the private sector in cybersecurity.

Key mechanisms for sharing threat information

There were four total networks that were discussed in the first two breakout groups. The first group looked at three existing networks that the participants felt were worthy of discussion—the OT-511 network for the trucking industry, the Rail Alert Network, and the Custom House Brokers Association. The second breakout group focused on the Oakland Domain Awareness Center (DAC) which is currently in the design and development phase (see Spotlight on P9.)

Participants looked at the collaborative capacity of the networks and identified the strengths and weakness of these systems in order to facilitate better understanding of how to improve local information sharing. The systems are described below.

OT-511

Valued Practice

The OT-511 Network is a text based system for sharing transportation related information (see spotlight on P3.) that has the potential to be used as a delivery system for all-hazards threat information. Participants noted that OT-511 is successful because it is a public/private partnership, is based on open source systems, and is relatively low cost.

Rail Alert Network

Valued Practice

The Rail Alert Network is sponsored by Association of American Railroads and is part of the national JTTF. Information on this network is proprietary and is privately funded. Railroad security is unique in that railroad police have both federal and state commissions, even though they are private organizations. The strength of this network is in its strong executive support, its ability to be secured, and its ease of implementation due to being based on existing systems.

Custom House Brokers Association Network

Valued Practice

The Custom House Brokers Association Network is a subscription based service that provides operational information to its members (Customs House Brokers). This information network is seen as a successful model for information sharing for several reasons. First, it has low operating costs because it is tied to membership dues. Second, it is targeted to a specific audience with specific business interests and clear responsibilities, even though it benefits multiple stakeholder types. Finally, it has a committed membership that is tied to a professional organization with a shared mission and altruistic values.

Oakland Domain Awareness Center

Valued Practice

The proposed joint city/port of Oakland Domain Awareness Center (DAC) will utilize the City of Oakland Emergency Operations Center (EOC) to consolidate a network of existing surveillance and security sensor data to actively monitor critical port facilities and related infrastructure. Threat security information will be collected, analyzed, and disseminated to facilitate prevention and response activities for both public and private stakeholders(see Spotlight on P9)

Spotlight: Domain Awareness Center

PORT OF OAKLAND

The Port of Oakland and City of Oakland are working jointly to establish a Domain Awareness Center (DAC), funded significantly by the American Recovery and Reinvestment Act of 2009. The DAC will be co-located with the City of Oakland's existing Emergency Operations Center (EOC) and provide the focal point for incident prevention and response coordination for the Port of Oakland.

Implementation

The DAC will consolidate a network of existing surveillance and security sensor data to actively monitor critical Port facilities, utility infrastructure, city facilities and roadways. Also planned are Information Technology improvements for increased security and resiliency. The Center will be expandable to provide a central coordination point for Maritime and Landside Domain Awareness for the San Francisco Bay region. It will link to the USCG and other agencies' local command centers and could also provide additional capabilities to other ports that are experiencing an emergency. The DAC plans to utilize information management software that would be utilized together with video analytics to screen and monitor data as well as coordinate incident management with dispatch and automated controls at specific facilities. The DAC will eventually operate 24/7 to provide coordination of prevention, preparedness, mitigation, response, and recovery efforts.

Development of the DAC is supported by the Domain Awareness and Response Coordination working group comprised of representatives from both the City of Oakland and the Port of Oakland. This group is using the following guidelines to improve domain awareness, prevention and response capabilities through the integration of efforts and interoperability among regional security partners:

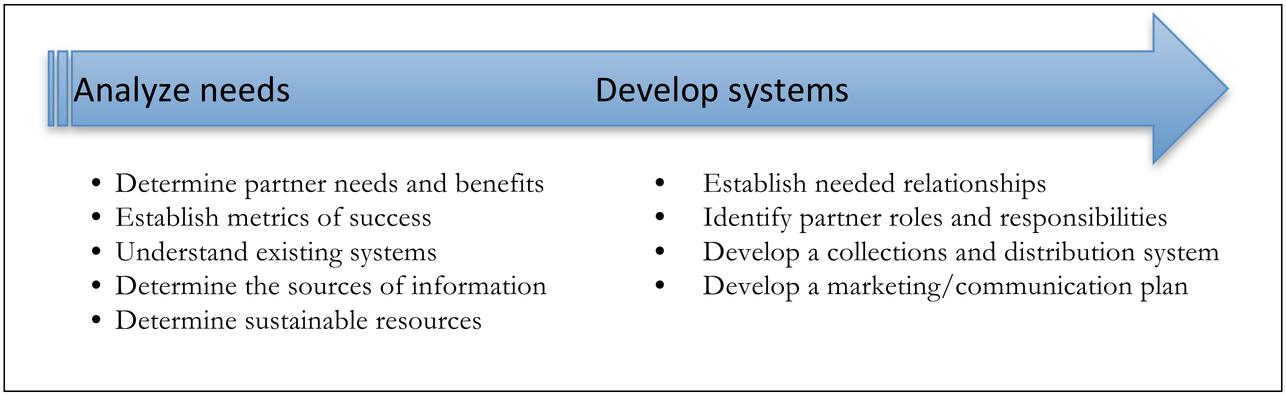
- Leveraging existing initiatives
- Strengthening linkages between existing command and control nodes
- Expansion of detection and deterrence capabilities
- Improving effective information management as a force multiplier
- Developing detailed Concept of Operations
- Enhancing immediate readiness capabilities
- Support National Preparedness Priorities
- Strengthen capabilities in Chemical, Biological, Radiological, Nuclear and Explosive Detection and Response

Impact

The integrated fiber optic system will allow for the assimilation, analysis, and dissemination of security information to maximize domain awareness within the Oakland region and facilitate the coordination of prevention and response activities in an emergency. To achieve domain awareness, information sharing will include risk potentials and threat trends that will facilitate decision making to mitigate risks and increase focus on prevention. The institutional framework for the DAC should facilitate and enhance new partnerships and coalitions and expand the already successful partnership of Oakland Police Department, Oakland Fire Department, the Office of Emergency Services and the Port of Oakland. New partnerships will include not only public agencies, but private sector stakeholders who rely on Port of Oakland to conduct business. As such, the DAC will support the San Francisco Bay Region Wide Risk Mitigation and Trade Resumption/Resiliency Plan (RM/TRRP).

Improving local networks

In the small group breakout sessions, the two groups that focused on local information sharing practices described a number of common themes regarding information sharing. Based on these discussions, the groups outlined future actions required for successful implementation of information sharing systems. As we reviewed the items targeted by the groups, a nine part process for designing information sharing networks surfaced. As shown in Figure 3, this process crosses over two phases of system design: analyzing needs and developing the system.



- Determine partner needs and benefits
- Establish metrics of success
- Understand existing systems
- Determine the sources of information
- Determine sustainable resources

- Establish needed relationships
- Identify partner roles and responsibilities
- Develop a collections and distribution system
- Develop a marketing/communication plan

Figure 2: System Roadmap

When it comes to sustainability, participants stressed the importance of both early analysis and targeted development of an information sharing system. These elements are discussed in detail below.

Analyze Needs

The first step for Oakland is to analyze the local environment by determining the partner needs and benefits, establishing metrics of success, understanding existing systems, determining the sources of information, and determining the necessary resources to sustain the program.

Determine partner needs and benefits

Participants noted the importance of first having a clear understanding of just what their stakeholders need to make the system easy to use, useful, and desirable.

Ease of Use

Participants felt that, in general, many of the systems out there were difficult to use. Although they did not identify any specific instances, they did identify factors that were seen to impact ease of use. These factors were the ability to access the information on multiple platforms (email, text, and web), the importance of tailoring, categorizing, and prioritizing information, and the importance of receiving information that is concise and timely. In addition, participants identified the need for secure systems that protect business intelligence.

For Oakland, the ease of accessing information was very important. Access issues included improving password policies, getting access to For Official Use Only (FOUO) information, and receiving adequate feedback when reporting. Participants first requested that Homeport extend password expiration times and provide clear and timely notifications on password expirations. Second, participants identified the local fusion center as a possible resource for easier access to FOUO information. Third, private sector participants noted the importance of receiving feedback when reporting. For example, there were incidents where thefts of containers were reported to multiple agencies (OPD, CHP, BEST) but the inter-agency reporting process was lengthy and the agencies did not provide feedback to the private sector on the results of the investigation. The private sector would like to receive follow-up information, which includes recommendations for how to proceed and information on lessons learned from the experience. Government participants also called for better communication between agencies.

For Oakland, the ease of accessing information was very important

Usefulness

As in our other ports, participants stressed the need for useful information. If industry receives useful information, it is not only easier for them to modify their security practices, it is also easier for them to justify the time and money spent on security. For our participants, useful information means seeing trends, mitigating risks, and learning from others. Trend information helps industry understand what to look out for and enables them to make better business decisions. For instance, being aware of upcoming protests can allow rail companies to divert trains away from the affected areas. Trend information empowers industry to do their job better—be 'proactive and not reactive', 'enable responsiveness', "protect cargo' and 'establish internal protocols.' Trend data can include crime information as well as information related to the overall threat picture, including suspicious behaviors, backups at terminals, and stolen containers.

In general, participants want to see trends, mitigate risks, and learn from others

Usefulness also means receiving information on risk patterns and hearing how specific threats could impact business planning and operating costs. They want to be able to research histories of events to help them predict areas of risk and recover more quickly from incidents.

Finally, usefulness includes the ability to collaborate with other ports and agencies. Participants want to see if there are similar problems in other ports and be aware of their lessons learned.

Desirability

Our Oakland participants stressed repeatedly the importance of getting buy-in to make the systems sustainable. Key to building buy-in is recognizing what is valued—what will motivate stakeholders to support and sustain a system. Our previous work, as shown in Figure 3) has uncovered how the sharing of information can benefit stakeholders in any of five arenas (the financial, operational, social, ideological, and strategic) and at any level of interaction (individual, group, organization, enterprise, or global.) These benefits can then be used to engage the commercial sector in financially supporting an information service. As discussed in the next section on value metrics, participants identified a number of ways to evaluate the success of an information sharing system that is based on providing value and increasing the desirability of sharing information.

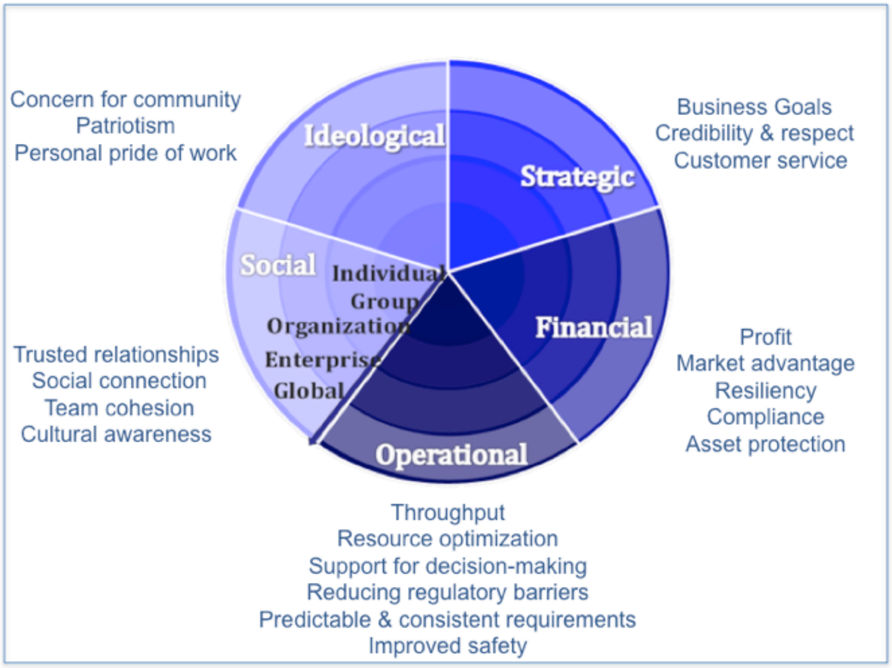


Figure 3: Stakeholder Values

Establish metrics of success

In Oakland, participants recognized the importance of establishing clear metrics for success prior to developing any new information system and the metrics should be based on stakeholder needs as discussed above. These metrics can be used for establishing objectives and measuring performance. For Oakland, the success criteria included measures of how well the system is used and how valuable the information is.

Value metrics

Participants felt that showing value was key to developing a sustainable system and they identified several metrics for evaluating the value of information sharing:

Financial & operational

- Lower costs
- Increased revenue
- Improved flow of commerce
- Increased risk mitigation

Strategic & Ideological

- Support business continuity
- Increased safety
- Lower crime
- Decreased pollution
- Better prepared for threats

Social

- Increased public confidence

Metrics can be used for establishing objectives and measuring performance

For our industry participants, risk mitigation was a key element—information systems that improve business planning and help reduce costs was highly valued and was seen as a good indicator for engaging the commercial sector.

As with the other ports studied, anything that has the potential to increase profits is important. Industry wants information that allows them to be proactive and make sure that commerce is flowing. Information is valuable when it helps industry improve security and increase safety.

Use metrics

Participants identified a number of metrics that could be used to gauge how well an information system is being used:

- Users are satisfied
- The mechanism is highly used (saturated)
- All users have access (wide coverage)
- There is comprehensive topic coverage
- Patterns of incidents are provided
- The information can be widely used

Understand existing systems

In looking at how to develop systems that are sustainable, participants noted that it is important to integrate existing information and mechanisms and not develop a brand new system. Whenever possible, information systems should tie in to existing platforms and be interoperable. Although we began identifying systems during the workshop, the participants recommended that this activity be continued prior to moving forward with creating another new system.

Determine the sources of information

Another factor that participants highlighted was the need to clearly understand what information is out there. Often, communities are not aware of all the options they have for receiving information. As part of this understanding, any needs analysis should first include a process for categorizing information source based on whether or not they are sharable, whether or not they are timely, and whether or not they are useful for operations. Secondly, participants felt that inconsistent and redundant information is prevalent. Inconsistent information leads to mistrust and results in a reduction in usage of the system. Duplications cause unnecessary work and result in additional costs. Redundant information is a major deterrent to the engagement of private sector partners.

Determine sustainable resources

The Oakland participants stressed the need for understanding and acting on issues that affect sustainability. Specifically, they recognized the risk of developing a system that lacks financial and operational support. To improve sustainability, this system should decrease or mitigate costs and demonstrate clear value.

The Oakland participants stressed the need for understanding and acting on issues that affect sustainability

First, to decrease costs, participants recommended that any new system leverage existing resources and be easy to integrate. The system should tie in to existing platforms and not create a new, incompatible network. They also want to be able to use existing personnel and resources. Finally, the integration should ensure that it is compatible with their existing security plans and requirements.

Second, sustainability relies on strong support from all stakeholders. A key aspect of gaining support is being able to demonstrate value to the commercial sector. For instance, truck drivers and dispatchers who see value in the information they receive from OT511 are willing to pay a fee. Similarly, an organization such as DAC is being initiated through public funds. As public budgets decrease, these organizations need to be able to translate their value into terms that private sector understand (e.g., costs mitigated by an early alert of potential delay that allowed rescheduling or redirection of shipments). This value can then be used to engage the commercial sector in financially supporting a service that improves their “bottom line.”

Develop the system

The second area that participants highlighted in designing an information sharing network is the need to define the resources and actions required for developing a system. Actions related to development include establishing needed relationships, clarifying partner roles and responsibilities, developing marketing and communication plans, and finally developing the collection and distribution system.

Establish needed relationships

The first step in developing a sustainable information sharing system is to establish needed relationships with key stakeholders. Participants felt that the MIST workshop was a useful structure for establishing and maintaining key relationships. To move information sharing efforts forward in the Bay Area, participants also want to make sure that they develop a strong commitment to participate in ongoing sharing . Future development efforts should focus on interlinking existing social networks, identifying key stakeholders and users, and establishing regular meetings to support a network of information sharing professionals.

Identify partner roles responsibilities

Our participants felt that an important part of the development of an information sharing system is the establishment of clear roles and policies. Roles should be clearly stated and responsibilities specified. The interest in bringing together information from different sources raises complex system integration challenges. To the extent that multiple organizations are concerned with different aspects of information collections, analysis, and dissemination (e.g., NCRIC, IOC, DAC) there is a need to clarify target areas and roles in order to assure complementarity and reduce redundancy. Another implementation challenge is potential or perceived "turf competition." This competition results from multiple organizations having a role in coordinated information sharing. In the Port of Oakland arena, these organizations include the USCG-led IOC, the NCRIC and the newly planned DAC.

An important part of the development of an information sharing system is the establishment of clear roles and policies

Participants felt that policies should also address the issue of overly restrictive information sharing policies. Government partners often are hesitant to share information because they are either 'handcuffed' by policies that limit sharing or perceive that there is not really a need to know on the part of the private sector. Government partners often struggle with balancing this need to know with the need to control information and be secure. There is a strong sense from both private and public partners that this hesitation results in 'overly secure' systems. Private sector stakeholders have some similar limitations in terms of sharing proprietary company information.

Develop a marketing/communication plan

Good communication with users and stakeholders was seen as an important step in increasing commitment and buy-in. Participants felt that it was important to build a shared mission and to show mutual benefit to the port, users, and the community. Some of the marketing challenges that were noted included continually changing memberships, and a lack of awareness of intermodal partners.

During this workshop, we had several private sector participants who were involved in local multipurpose networks on a daily basis. These participants pointed out that successful information sharing systems require significant marketing and outreach. This outreach is critical in building ongoing support for information sharing and requires a clear demonstration of benefits. For example, because the Port of Oakland is the largest source of revenue for the City of Oakland, communicating the positive impact on the flow of commerce will build buy-in for both commercial and local government agencies. Another benefit that can build buy-in is communicating the impact of programs (such as the DAC and OT-511) on the Port's overall security posture (as demonstrated by the DAC support from Port Security Grant funding (from DHS) and the Bay Area UASI (Bay Area Security Initiative).

It is important to build a shared mission and show mutual benefit to the port, the users, and the community

In addition, there are logistical challenges involved in building user support that can benefit from a more focused marketing effort. In particular, the OT-511 program has had difficulty expanding their membership due to the perceived technical difficulties of enrolling in the texting service. The DAC as well needs to gain the engagement of critical public and private sector partners. This might initially be addressed through a marketing approach, but will ultimately require the development of something more formal like a Memorandum of Agreement (MOA) that specifies the relationship among the participating organizations.

Develop a collections and distribution method

Finally, participants sought to achieve an integrated, distributed information system that includes both collection and distribution arms. This system should be easily maintained and increase efficiencies rather than increase work. One important improvement identified by workshop participants is a mechanism for sharing unclassified information that may be embedded in otherwise classified, or limited distribution documents. This was referred to as 'establishing a tear line' that would allow information valuable to achieving the impacts listed above to be disseminated. Such a process would require negotiated "rules" and agreements among participating organizations about how decisions would be made regarding what would be above the tear line (restricted) and what would be below the tear line and how the latter would be disseminated.

Cybersecurity

As noted earlier the third breakout group addressed the topic of cybersecurity. This idea of cybersecurity surfaced as a possible small group topic for the Oakland MIST workshop at a prior Harbor Safety Committee meeting. This topic became even more relevant with the release of the *Executive Order on Improving Critical Infrastructure Cybersecurity* on February 12, 2013[12]. Sections 4 and 7 of this order address the needed information sharing elements and the alignment of business and technological approaches. Section 4 specifically states that "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." Section 7 calls for the development of a "Cybersecurity Framework (that) shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."

The role of cyber security

The small group activity began with trying to define, "what is cybersecurity in terms of the multimodal global supply chain?" Is the scope simply to address vulnerabilities on the information sharing systems or are we also addressing vulnerabilities in control systems? The group felt that cybersecurity was in the wheelhouse of information technology and that IT professionals need to be included in the discussion of these questions. Realizing that the workshop participants were primarily operational planners and physical security professionals, we engaged in an initial discussion of the role of cybersecurity. As a result of this discussion, we identified three elements at play in improving cybersecurity in the supply chain.

We need to increase coordination between our physical security operations and information technology

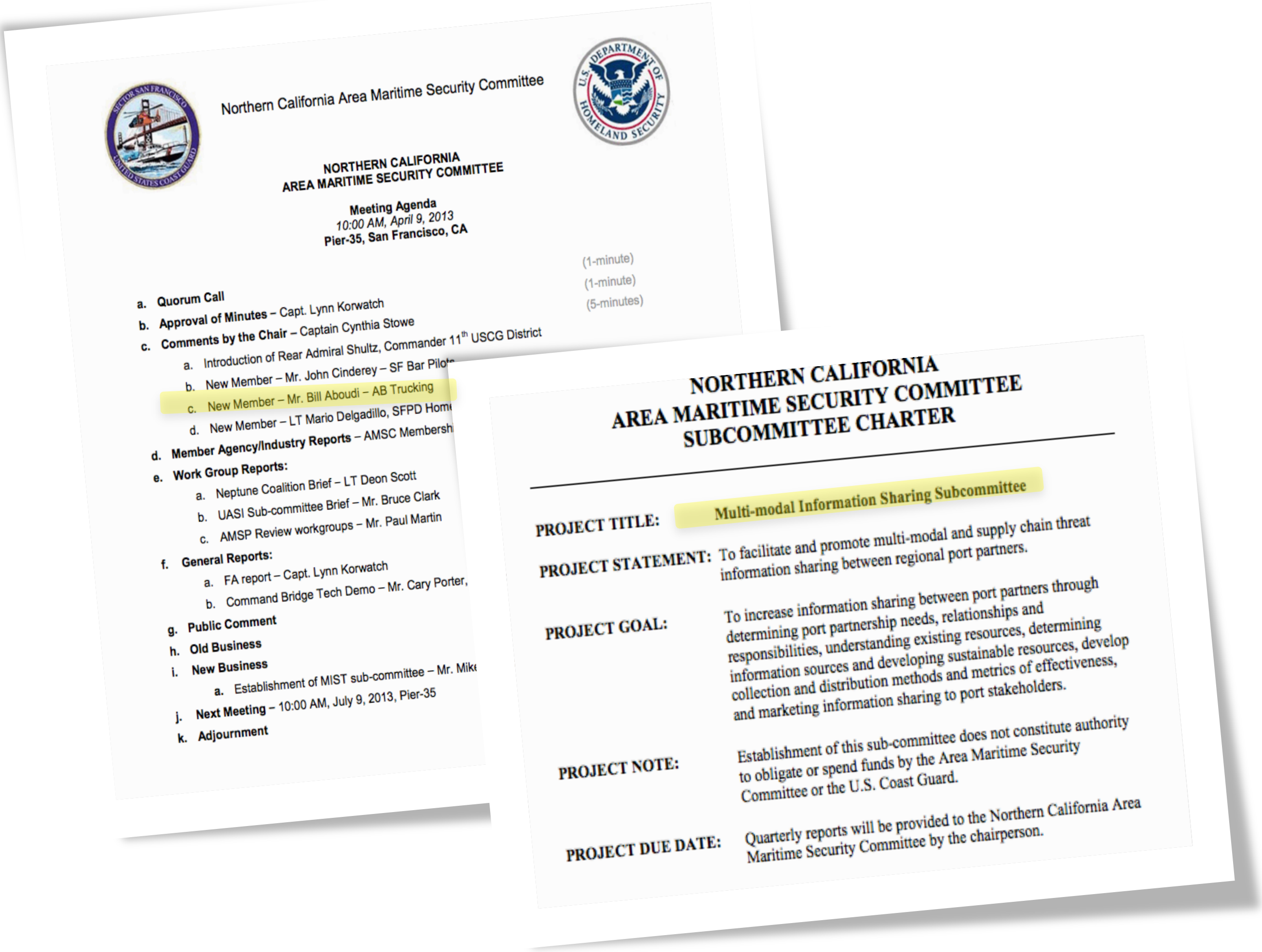
First, government systems are fragmented. The situational awareness databases from the CBP, USCG, FBI and local law enforcement are not connected. This fragmentation is compounded by a belief that in opening up systems to share, even between trusted partners, the systems will be more vulnerable to attacks. This issue of fragmented and compartmentalized mechanisms negatively impacts an organizations ability to share critical threat and security information safely.

Secondly, we need to understand where our cybersecurity risks are and establish standards for information sharing. For instance, does accessing social networking sites raise our systems vulnerabilities? Is the practice of having 'dirty' computers to access outside the firewall providing any mitigation? Are our security measures slowing down our access to critical threat information?

Lastly, we need to increase our coordination between our physical security operations and information technology security operations. IT security professionals have been focused on firewalls, encryption and access, while operations professionals are doing their best to be up-to-date on information assurance practices and compliance. Industry depends on both groups of professionals to help them to keep business flowing while fighting this 'invisible' enemy. As the amount of data grows and attacks become more elegant we need to work closely to ensure that we are gaining real defense and not at too great of an expense for industry.

Outcomes

As the participants discussed both the proposed and existing mechanisms for information sharing, they determined that there was a need to continue this conversation in a more formalized way. The participants outlined a process for moving their efforts forward resulting in a roadmap for developing information sharing systems (discussed in the next section), the creation of a Maritime Information Sharing Subcommittee to the local Area Maritime Security Committee (AMSC) formally created in April 2013 (see Figure 4), and the inclusion of multimodal partners in the AMSC (a trucking industry representative was sworn in on April 9, 2013.)



Northern California Area Maritime Security Committee

NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE

Meeting Agenda
10:00 AM, April 9, 2013
Pier-35, San Francisco, CA

a. **Quorum Call** (1-minute)
b. **Approval of Minutes** – Capt. Lynn Korwatch (1-minute)
c. **Comments by the Chair** – Captain Cynthia Stowe (5-minutes)
    a. Introduction of Rear Admiral Shultz, Commander 11th USCG District
    b. New Member – Mr. John Cinderey – SF Bar Pilots
    c. New Member – Mr. Bill Aboudi – AB Trucking
    d. New Member – LT Mario Delgadillo, SFPD Home
d. **Member Agency/Industry Reports** – AMSC Membershi
e. **Work Group Reports:**
    a. Neptune Coalition Brief – LT Deon Scott
    b. UASI Sub-committee Brief – Mr. Bruce Clark
    c. AMSP Review workgroups – Mr. Paul Martin
f. **General Reports:**
    a. FA report – Capt. Lynn Korwatch
    b. Command Bridge Tech Demo – Mr. Cary Porter,
g. **Public Comment**
h. **Old Business**
i. **New Business**
    a. Establishment of MIST sub-committee – Mr. Mike
j. **Next Meeting** – 10:00 AM, July 9, 2013, Pier-35
k. **Adjournment**

NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
SUBCOMMITTEE CHARTER

PROJECT TITLE: Multi-modal Information Sharing Subcommittee

PROJECT STATEMENT: To facilitate and promote multi-modal and supply chain threat information sharing between regional port partners.

PROJECT GOAL: To increase information sharing between port partners through determining port partnership needs, relationships and responsibilities, understanding existing resources, determining information sources and developing sustainable resources, develop collection and distribution methods and metrics of effectiveness, and marketing information sharing to port stakeholders.

PROJECT NOTE: Establishment of this sub-committee does not constitute authority to obligate or spend funds by the Area Maritime Security Committee or the U.S. Coast Guard.

PROJECT DUE DATE: Quarterly reports will be provided to the Northern California Area Maritime Security Committee by the chairperson.

Figure 4: The new AMSC Charter

Appendix A: List of acronyms

AMSC	Area Maritime Security Committee
CBP	U.S. Customs and Border Protection
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
FBI	Federal Bureau of Investigation
IOC	Interagency operation center
JTTF	Joint Terrorism Task Force
MARAD	U.S. Department of Transportation Maritime Administration
MIST	Multimodal Information Sharing Team
NPS	Naval Postgraduate School
UASI	Urban Area Security Initiative
USCG	U.S. Coast Guard

Appendix B: Regional Resources

Programs & Centers

California Maritime Academy: www.csum.edu

Located in Vallejo, California, The California Maritime Academy (Cal Maritime) is a unique and specialized campus of the 23-campus California State University (CSU) system. We are one of only seven degree-granting maritime academies in the United States — and the only one on the West Coast.

Joint Terrorism Task Force (JTTF):

The San Francisco Division of the Federal Bureau Investigation JTTF brings together federal agents and local/state law enforcement officers throughout the Bay area to collaboratively work to investigate and prevent acts of terrorism. By pooling wide-ranging expertise and resources, the JTTF is more effective and efficient than any single agency working alone. The JTTF facilitates the collection and sharing of timely, vetted intelligence both with local agencies and with the larger U.S. intelligence community. This proactive collaboration allows JTTF members to quickly identify emerging threats and mobilize resources to disrupt terrorist activities.

Northern California Regional Intelligence Center (NCRIC): www.ncric.org

The Northern California Regional Intelligence Center (NCRIC) helps safeguard the community by serving as a dynamic security nexus. To detect, prevent, investigate and respond to criminal and terrorist activity, the NCRIC disseminates intelligence and facilitates communications between Federal, State and local agencies and private sector partners to help them take action on threats and public safety issues. The NCRIC disseminates intelligence products such as the NCRIC Partner Update Brief.

West State Alliance: www.weststate.org

West State Alliance (WSA) was founded as a nonprofit trade association in 2004 by a dedicated group of independent trucking companies serving the Port of Oakland. As a trade association, WSA represents the interests of independent trucking companies in their business relationships with steamship and stevedoring companies operating in West Coast ports of the United States. While promoting the highest standards for safe, efficient and environmentally conscious containerized transportation, WSA advocates for and promotes legislative, regulatory and economic priorities favorable to small business and the transportation industry. Likewise, as a membership organization, WSA strives to ensure conditions that support fair and equitable treatment of independent truckers.

Working Groups

There are several working groups in the region such as FSOs that meet regularly through the Port of Oakland, and working groups created to address a particular threat such as the Copper Theft Working Group. The following is a catalog of some of the more formal stakeholder working groups.

Cargo Theft Interdiction Team (CTIP): http://www.chp.ca.gov/programs/ctip.html

With the growing number of cargo thefts statewide, an alliance has been established between law enforcement and private industry to maintain open lines of communication. Organizations such as the Western States Cargo Theft Association, American Trucking Association, California Trucking Association and National Cargo and Security Council. Transportation company security directors and law enforcement personnel, meet on a monthly basis to discuss recent trends, losses, suspects, and active investigations. This type of partnership is the foundation of successful cargo theft enforcement.

Harbor Safety Committee: http://www.sfmx.org/support/hsc/

In 1990, The California State Legislature enacted the Oil Spill Prevention and Response Act (OSPRA). The Act (SB 2040) created harbor safety committees for the major harbors of the State of California to plan "for the safe navigation and operation of tankers, barges, and other vessels within each harbor...(by preparing)...a harbor safety plan, encompassing all vessel traffic within the harbor." The full committee for the Harbor Safety Committee holds regular monthly public meetings. The San Francisco Harbor Safety Plan encompasses a series of connecting bays, including the San Francisco, San Pablo and Suisun Bays, and the Sacramento River to the Port of Sacramento and the San Joaquin River to the Port of Stockton.

Neptune Coalition:

The Neptune Coalition is composed of 20 participating Bay Area law enforcement and emergency response agencies with maritime assets, and is a cooperative effort to enhance the safety and security of the ports within the Bay Area and Delta. The Coalition accomplishes this primary objective through monthly meetings, joint training and law enforcement operations, and participation in annual marine events such as Navy Fleet Week. The mission of the Neptune Coalition is to bring to bear all the available maritime public safety resources in the Greater San Francisco Bay and River Delta Area in a concerted effort to enhance the safety and security of the ports and the general public within the Bay Area.

Northern California Area Maritime Security Committee (AMSC):

The mission of this Area Maritime Security Committee is to help coordinate planning, information sharing, and other necessary activities to aid the security of the Marine Transportation System (MTS). The geographic boundaries of this Committee include the entire Captain of the Port San Francisco area of responsibility.

Trade Facilitation Committee: http://www.sfmx.org/support/tfc/

The San Francisco Marine Exchange Trade Facilitation Committee brings together in an informal structure representatives from the USCG, CBP, MARAD, insurers, attorneys, freight forwarders, customs brokers, ports, carriers, stevedores, bankers, Congress, and the Senate. The objective, as stated by its name, is to provide assistance, ease, support, and mitigation; to disentangle, extricate, increase accessibility, manage, influence, and promote and facilitate trade.

Trucker Working Group: http://www.weststatealliance.shuttlepod.org/

West State Alliance founded the Trucker Work Group (TWG) in 2007 as the result of an initiative by independent truckers to improve relations with Port of Oakland administration. The group is co-chaired by a representative each from the Port and from the trucking industry who together select program topics and speakers.

Private Sector Stakeholders

ASIS: http://www.sfasis.org/Default.asp

The American Society for Industrial Security (ASIS) International is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests. The San Francisco Bay Area Chapter is one of the founding chapters of ASIS and is one of the largest ASIS Chapters worldwide. Membership represents the entire spectrum of security professionals including managers and directors of security from many Fortune 500 companies.

California Trucking Association: http://caltrux.org/

The California Trucking Association promotes leadership in the California motor carrier industry, advocates sound transportation policies to all levels of government, and works to maintain a safe, environmentally responsible and efficient California transportation goods movement system.

Customs Brokers and Forwarders Association of Northern California: www.cbfanc.org

The Customs Brokers and Forwarders Association of Northern California (CBFANC) is an industry association that focuses on improving standards of conduct and services; highlighting innovations, trends, and regulatory changes which may affect members' clients, and taking common action when necessary. The regional association, which serves all of Northern California, is an active and voting member of the Pacific Coast Council of Customs Brokers and Forwarders Associations (PCC) and is also an affiliate of the National Customs Brokers and Forwarders Association of America (NCBFAA). The volunteer board and committee chairs cooperate with local Customs & Border Protection, the U.S. Department of Agriculture, the Food & Drug Administration and Fish & Wildlife to ensure that goods and services flow seamlessly across our borders.

Marine Exchange of the San Francisco Bay Region: http://www.sfmx.org/

The Marine Exchange of the San Francisco Bay Region is a non-profit, membership organization. The collection, analysis, and dissemination of ship traffic information for the Golden Gate maritime community has been the primary purpose of the Marine Exchange since 1849.

Oakland Maritime Support Services (OMSS): http://www.oaklandmss.com/

Co-located at central location OMSS provides a range of support services for trucking companies that serve the Port of Oakland. OMSS will also contribute to local economic prosperity and minimize the impact of truck traffic to the West Oakland Community.

Pacific Maritime Association (PMA): www.pmanet.org

The principal business of the Pacific Maritime Association is to negotiate and administer maritime labor agreements with the International Long shore and Warehouse Union. Member companies are cargo carriers, terminal operators and stevedores that operate at West Coast ports, where overall cargo movement supports 8 million U.S. jobs. PMA also hosts regular meetings of FSOs in the Port of Oakland.

The Pacific Merchant Shipping Association (PMSA): http://www.pmsaship.com/

The PMSA is an independent, not-for-profit association focused on global trade. PMSA operates offices in San Francisco, Long Beach and Seattle, and represents owners and operators of marine terminals and U.S. and foreign vessels operating throughout the world. On behalf of its members, PMSA engages in community affairs and legislative and regulatory affairs in California and Washington state. PMSA provides members with information services, including regular updates on matters of interest to the shipping industry. It also serves as a clearinghouse for environmental practices across the industry.

San Francisco Bar Pilots: http://sfbarpilots.com/

The San Francisco Bar Pilots regularly compile recommended guidelines for safe navigation entitled, Port safety Guidelines for Movement of Vessels of San Francisco Bay and Tributaries. The guidelines are sent to members of the shipping industry and are based on a general consensus among pilots as to recommended navigational practices. The San Francisco Bar Pilots partner closely with the United States Department of Homeland Security, the U.S. Coast Guard and other law enforcement agencies to ensure maritime security. Thirty two of the Coast Guard's 37 identified critical security locations in Northern California are within the San Francisco Bar Pilots' jurisdiction, and their presence on board performs an important security function.

Public Sector Stakeholders

Port of Oakland: http://www.portofoakland.com/

The Port is an independent department of the City of Oakland, and acts as trustee on behalf of the State for all Port property. Governed by a Board of Port Commissioners, nominated by the mayor of Oakland and appointed by a vote of the City Council, the Port of Oakland funds its own operations. It receives no tax money from the City of Oakland and the State of California.

Oakland Fire Department (OFD): http://www2.oaklandnet.com/Government/o/OFD/index.htm

The mission of the Oakland Fire Department to implement comprehensive strategies and training in fire prevention, fire suppression, emergency medical services, and all risk mitigation, including: human-caused and natural disasters, emergency preparedness, 9-1-1 services and community-based fire services.

Oakland Emergency Management Services Division (EMSD):http://www2.oaklandnet.com/Government/o/OFD/o/OES/index.htm

The OFD Emergency Management Services Division (EMSD) coordinates the activities of all City agencies relating to planning, preparation and implementation of the City's Emergency Plan. EMSD also supports the coordination of the response efforts of Oakland's Police, Fire and other first responders in the City's state-of-the-art Emergency Operations Center to ensure maximum results for responders, the ability to provide up-to-date public information and the ability to provide the best resource management during a crisis. Additionally, EMSD coordinates with the Operational Area and other partner agencies to guarantee the seamless integration of federal, state and private resources into local response and recovery operations.

Oakland Police Department (OPD): http://www2.oaklandnet.com/Government/o/OPD/index.htm

The mission of the Oakland Police Department (OPD) is to provide the people of Oakland an environment where they can live, work, play, and thrive free from crime and the fear of crime. The work of the Oakland Police Department is handled by different groups within the Department: sworn and reserve officers, cadets, and civilian employees.

Port of San Francisco: http://www.sfport.com/

The Port of San Francisco is a public agency responsible for managing seven and one half miles of San Francisco Bay, which the Port develops, markets, leases, administers, manages, and maintains. The Port's responsibilities include promoting maritime commerce, navigation, and fisheries; restoring the environment; and providing public recreation. The Port of San Francisco is governed by a five member Board of Commissioners, each of whom is appointed by the Mayor and subject to confirmation by the City's Board of Supervisors. Each commissioner is appointed to a four-year term.

San Francisco Department of Emergency Management (DEM): http://sfdem.org/

The San Francisco Department of Emergency Management (DEM) manages disaster preparation, mitigation, and response; 9-1-1 dispatch; and homeland security grant distribution for the City and County of San Francisco. DEM was created in 2006 by local legislation that reorganized the Emergency Communications Department and the Office of Emergency Services into a single agency. DEM is composed of two divisions: Emergency Communications and Emergency Services.

San Francisco Fire Department (SFFD): http://www.sf-fire.org/

The San Francisco Fire Department serves an estimated 1.5 million people, providing fire suppression and emergency medical services to the residents, visitors and workers within San Francisco's 49 square miles.

San Francisco Police Department (SFPD): http://sanfranciscopolice.org/

The San Francisco Police Department (SFPD) is comprised of over 2000 officers serving in ten stations located throughout the city. The SFPD community policing program, from community meetings to Citizen's Police Academy, builds an ongoing working relationship between officers and the communities they serve that makes policing work.

Regional/State

Alameda Sheriff's Department Marine Patrol Police Unit: https://www.alamedacountysheriff.org/les_contracts.php

The Alameda County Sheriff's Office primary mission is to act as a deterrent to possible terrorist attacks on the Port of Oakland and within the San Francisco Bay, and is charged with ensuring the safety and security of the waterways that are located throughout the County of Alameda. The multi-mission Marine Patrol Unit operates throughout the County's waterways and assists other local, State, and Federal agencies, as well as military assets, in all facets of marine operations. Marine Patrol Unit programs include: 1) marine patrol boats, 2) personal watercraft response unit, and 3) underwater explosive recovery team.

Bay Planning Coalition (BPC): http://bayplanningcoalition.org/about/

The mission of the Bay Planning Coalition (BPC) is to work through a broad coalition, which will enhance the quality of life in the San Francisco Bay Region. BPC work focuses on advocacy, monitoring and partnering with other associations who recognize the need for fair and reasonable regulation and sound, integrated planning.

California Emergency Management Agency (Coleman): http://www.calema.ca.gov/Pages/default.aspx

The California Emergency Management Agency exists to enhance safety and preparedness in California through strong leadership, collaboration, and meaningful partnerships. Our mission is founded in public service. Our goal is to protect lives and property by effectively preparing for, preventing, responding to, and recovering from all threats, crimes, hazards, and emergencies.

California Highway Patrol (CHP): http://www.chp.ca.gov/

The mission of the California Highway Patrol is to provide the highest level of safety, service, and security to the people of California. This is accomplished through five departmental goals: 1) prevent loss of life, injuries, and property damage; 2) maximize service to the public and assistance to allied agencies; 3) manage traffic and emergency incidents: 4) protect public and state assets; and 5) improve departmental efficiency.

California State Lands Commission: http://www.slc.ca.gov/

The mission of the California State Lands Commission is to serve the people of California by providing stewardship of the lands, waterways, and resources entrusted to its care through economic development, protection, preservation, and restoration.

California Board of Pilot Commissioners: http://www.bopc.ca.gov/

The Board of Pilot Commissioners for the Bays of San Francisco, San Pablo and Suisun (Board or BOPC) – sometimes called the "the Pilot Commission" – licenses and regulates up to 60 pilots who guide ships in the Bays of San Francisco. The licensed pilots are organized for business operational purposes as the "San Francisco Bar Pilots". Currently made up of seven members appointed by the Governor of California, the Board was created by the first legislative session of the new state of California in 1850 and has been serving continuously ever since.

Golden Gate Ferry: http://goldengateferry.org/

The Golden Gate Bridge, Highway and Transportation District operates the Golden Gate Bridge and two public transit systems: 1) Golden Gate Transit buses and 2) Golden Gate Ferry. Last year, 38 million vehicles crossed the Golden Gate Bridge and over 9 million customers rode the transit systems.

Lawrence Livermore National Lab (LLNL): https://www.llnl.gov/index.html

Lawrence Livermore National Laboratory has a mission of strengthening the United States' security through development and application of world-class science and technology to: 1) enhance the nation's defense; 2) reduce the global threat from terrorism and weapons of mass destruction; and 3) respond with vision, quality, integrity and technical excellence to scientific issues of national importance.

Metropolitan Transportation Commission (MTC): http://www.mtc.ca.gov/

The Metropolitan Transportation Commission (MTC) functions as both the regional transportation planning agency — a state designation — and, for federal purposes, as the region's metropolitan planning organization (MPO). As such, it is responsible for regularly updating the Regional Transportation Plan, a comprehensive blueprint for the development of mass transit, highway, airport, seaport, railroad, bicycle and pedestrian facilities.

Port of Richmond: http://www.ci.richmond.ca.us/index.aspx?nid=102

The Port of Richmond is approximately nine miles from the Golden Gate on the east shore of San Francisco Bay and is easily accessible by a federally-maintained deep water channel, the Richmond Harbor Channel. Richmond is served by the interstate highway system and two major transcontinental railroads – Burlington Northern Santa Fe and Union Pacific. Richmond has 32 miles of shoreline along the northern and eastern reaches of San Francisco Bay. There are five city-owned terminals. These tenant-operated terminals handle a wide range of liquid and dry bulk commodities, automobiles, and diversified cargo. The Port of Richmond also encompasses ten privately owned terminals for handling bulk liquid, dry bulk materials, metals, and break-bulk cargoes.

Federal

Border Enforcement Security Task Force (BEST): http://www.ice.gov/best/

In 2005, in response to the significant increase in violence along the Southwest Border in Mexico, the U.S Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), in partnership with U.S. Customs and Border Protection (CBP), as well as other federal, state, local, and international law enforcement officials created the Border Enforcement Security Task Force (BEST) in Laredo, Texas. To date, a total of 35 BESTs have been initiated across sixteen states and in Puerto Rico. These teams are comprised of over 750 members who represent over 100 law enforcement agencies who have jointly committed to investigate transnational criminal activity along the Southwest and Northern Borders and at domestic seaports.

Customs and Border Protection (CBP): http://www.cbp.gov/

Customs and Border Protection (CBP) is part of the Department of Homeland (DHS) with a priority mission of keeping terrorists and their weapons out of the U.S. CBP also has a responsibility for securing the border and facilitating lawful international trade and travel while enforcing hundreds of U.S. laws and regulations, including immigration and drug laws.

Department of Homeland Security (DHS): http://www.dhs.gov/

The Department of Homeland Security (DHS) combined 22 different federal departments and agencies into a unified, integrated cabinet agency when it was established in 2002. DHS missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience.

Department of Transportation (DOT): http://www.dot.gov/

The Department of Transportation (DOT) was established by an act of Congress on October 15, 1966 with the stated mission 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/

Established by legislation in 1988, the Federal Emergency Management Agency (FEMA) has over 7,000 employees across the nation – at Headquarters, the ten regional offices, the National Emergency Training Center, Center for Domestic Preparedness/Noble Training Center and other locations. FEMA's mission is to support U.S. citizens and first responders to ensure that the nation works together to build, sustain and improve capabilities to prepare for, protect against, respond to, recover from and mitigate all hazards.

Federal Bureau of Investigation (FBI) San Francisco Field Division: http://www.fbi.gov/sanfrancisco

As an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the Federal Bureau of Investigation (FBI) is to protect and defend the U.S. 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.

Immigration and Customs Enforcement (ICE): http://www.ice.gov/

Immigration and Customs Enforcement is the principal investigative arm of the 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 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://www.ise.gov/

The ISE provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep our people safe. The ISE Program Manager (PM-ISE) brings together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. The primary focus is any mission process, anywhere in the U.S., that is intended or is likely to have a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity.

Maritime Administration (MARAD): http://www.marad.dot.gov/

The Maritime Administration (MARAD) is the agency within the Department of Transportation (DOT) dealing with waterborne transportation. Its programs promote the use of waterborne transportation and its seamless integration with other segments of the transportation system. MARAD works in many areas involving ships and shipping, shipbuilding, port operations, vessel operations, national security, environment, and safety.

National Oceanic and Atmospheric Administration (NOAA): http://www.noaa.gov/

With a vision of "Science, Service, and Stewardship", the mission of the National Oceanic and Atmospheric Administration (NOAA) is to 1) understand and predict changes in climate, weather, oceans, and coasts; 2) share that knowledge and information with others; and 3) conserve and manage coastal and marine ecosystems and resources.

U.S. Coast Guard (USCG): http://www.uscg.mil/

With over 43,000 active duty members, 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.

U.S. Navy (USN): http://www.navy.mil/

With nearly 320,000 active duty members, the mission of the U.S. Navy (USN) is to maintain, train and equip combat-ready Naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas.

National Maritime Intelligence Office (NMIO): http://www.nmic.gov/

The National Maritime Intelligence-Integration Office (NMIO) is the unified maritime voice of the United States 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. The goal of NMIO is to enable maritime stakeholders to proactively identify, locate, and track threats to the interests of the U.S. and its global partners.

Information Systems

FORMAL

Homeland Security Information Network (HSIN):

The Homeland Security Information Network (HSIN) is a national secure web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

Homeport (USCG): https://homport.uscg.mil

Homeport is the web-based information sharing tool of the U.S. Coast Guard. The basic level of information is publicly accessible, and higher levels are access controlled and only accessible to a vetted list of stakeholders.

InfraGard (FBI): https://www.sfbay-infragard.org/

InfraGard is a unique national partnership between the private sector and the U.S. government represented by the Federal Bureau of Investigation (FBI). The San Francisco Bay Area InfraGard Chapter established in partnership with the FBI San Francisco Division is one of 85 chapters in the FBI's InfraGard network and a member of the InfraGard National Members Alliance.

Maritime Information Service of North America (MISNA): http://www.misnadata.org/

Maritime Information Services of North America (MISNA) is a coalition of non-profit maritime information service organizations dedicated to providing information, communications and related services to ensure safe, secure, efficient and environmentally sound maritime operations. MISNA membership includes maritime exchanges and associations from throughout the United States, Canada and Europe.

National Suspicious Activity Report (SAR):

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort led by the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, in partnership with the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

OT-411:

OT-411 is the Oakland Trucker Information Center located at 11 Burma Road in Oakland. The facility is maintained and operated by the OMSS

OT-511:

OT-511 is the Port Traffic Information System, a series of Twitter to text information feed for truckers operated by West State Alliance and sponsored by the MTC and the Port of Oakland.

"See something, Say something" (DHS):

In July 2010, the Department of Homeland Security (DHS) launched a national "If You See Something, Say Something™" campaign is a simple and effective program to engage the public and key frontline employees to identify and report indicators of terrorism and terrorism-related crime to the proper transportation and law enforcement authorities. DHS launched the "If You See Something, Say Something™" campaign in conjunction with the Department of Justice's Nationwide Suspicious Activity Reporting 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 Federal Bureau of Investigation-led Joint Terrorism Task Forces for further investigation and Fusion Centers for analysis.

WatchKeeper (USCG):

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. The heart of the IOC is the WatchKeeper information sharing and management system software. WatchKeeper coordinates and organizes port security information to help DHS and federal, state and local maritime partners make the best use of their resources.

Informal

In addition to formal information sharing systems, there is an array of informal communication channels used by regional stakeholders. These informal communication methods include, but are not limited to:

- Email
- Face-to-face conversations
- Instant messaging
- Internet
- Google alert
- Proprietary systems
- Tabletop exercises
- Telephone
- Text
- Yahoo group

Appendix C: References

[1] Salem, Anita, Hocevar, S.P., Wendy Walsh and Lyla Englehorn (2011). "MIST Summary of Findings 2008 2012 (narrated). Last accessed 29 May 2013 at http://www.youtube.com/user/MISTnps

[2] 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 May 2013 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-LongBeach%202008.pdf

[3] 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 29 May 2013 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-PugetPound202009.pdf

[4] 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 29 May 2013 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Delaware20Bay202010.pdf

[5] 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 29 May 2013 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Honolulu202010.pdf

[6] 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 29 May 2013 at http://www.nps.edu/Academics/Schools/GSBPP/docs/CDMR/MIST-Boston202011.pdf

[7] Hocevar, Susan Page, Jansen, Erik, Thomas, Gail Fann (2011) Inter-Organizational Collaboration: Addressing the Challenge. *Homeland Security Affairs*, September 2011. http://www.hsaj.org/?article=7.2.5

[8] United States Government Accountability Office, December 2002 *** Do we know the title or # of this report? If it's one I've cited, I think the GAO reports I used related to collaboration are more recent than 2002. Here's one of 2 I think are relevant (and support the statement in the text of the report):
United States Government Accountability Office (2010). National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration, GAO-10-822T

[9] Granovetter, M.S. (1973). "The Strength of Weak Ties", *Amer. J. of Sociology, Vol. 78, Issue 6, May 1360-80.*

[10] Malcolm Gladwell (200). The Tipping Point: How Little Things Can Make a Big Difference. Little Brown. ISBN 0-316-31696-2

[11] Barabasi, Albert-Laszlo (2003). *Linked - How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. Plume. ISBN 0-452-28439-2.

[12] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity