GLOBAL MARITIME INFORMATION SHARING SYMPOSIUM 2009

September 15—17
National Defense University
Fort Lesley J. McNair
Washington, D.C., USA

Aligning government outreach to the maritime industry. Bringing the industry perspective into government policy.

www.gmsa.gov/gmiss

Foreword

On behalf of the Office of Global Maritime Situational Awareness and our partner agencies and organizations, I am pleased to present this summary report of the second annual Global Maritime Information Sharing Symposium to the global maritime community of interest.

Making this symposium a success involved the work, resources, and expertise of several organizations. Once again, I would like to thank the Maritime Administration, the Department of Justice Office of Community Oriented Policing Services, the staff of U.S. Coast Guard Headquarters, the Office of the Director of National Intelligence, the National Maritime Intelligence Center, U.S. Fleet Forces Command, Naval Cooperation and Guidance for Shipping, the Naval Postgraduate School, and the National Defense University, without whose involvement the success of GMISS 2009 would have been diminished.

Equally important to the outcome of GMISS 2009 were the more than 40 speakers, presenters and panelists. A shared understanding of the broad range of perspectives represented within the maritime community enabled participants to reach general consensus on a number of complex and controversial issues within the time limits of the symposium. I am grateful to our speakers for their knowledge and experience, and for their courage in speaking plainly about topics that can at times generate some very heated discussion.

Most importantly, the organizers of GMISS want to thank each participant who took time away from his or her primary concerns to spend three days helping us move several critical issues forward. The true meaning of your decision to come and contribute so much of your time within this difficult economic climate is genuinely understood and appreciated.

That said, I ask you to help us bring to resolution the issues raised at GMISS by joining us in our ongoing working groups. Much work remains to be accomplished. The maritime awareness policy decisions the government makes impact both the maritime industry and the global supply chain for which it is the lynchpin. Your knowledge and expertise are necessary to ensure these decisions capitalize on the full measure of the industry's potential contribution to maritime awareness, and are informed by a reasonable understanding of this incredibly complex system of systems.

Thank you again, and we look forward to seeing you at GMISS 2010 next summer.

Gary Seffel

Director
Office of Global Maritime Situational Awareness

Table of Contents

Foreword i

Table of Contents ii

I. Overview I-1

Background I-1

GMISS Structure I-7

GMISS – MIST Partnership I-7

GMISS 2009 ..... I-8

II. Summary of Proceedings II-1

Recurring Themes II-1

Working Group Results II-4

Shared Priorities Inferred from GMISS Working Groups II-6

III. Ongoing Working Groups III-1

GMISS Working Group A: The Information Grid Working Group III-1

GMISS Working Group B: The Understanding Gap Working Group III-2

GMISS Working Group C: The Information Safeguards Working Group III-3

GMISS Working Group D: Operational Collaboration Model Working Group III-4

Return to Action III-5

IV. Appendices IV-1

A. OGMSA Background

B. Maritime Domain Awareness Enterprise Hubs

C. GMISS 2009 Agenda

D. Summary of GMISS 2009 Presentations

E. Recurring Themes during GMISS Sessions

F. GMISS Working Group Common Conclusions

G. GMISS 2008 Executive Summary

H. 2009 MIST (Puget Sound) Executive Summary

I. Overview

The second annual Global Maritime Information Sharing Symposium (GMISS) was held September 15th through 17th, 2009 at the National Defense University on Fort Lesley J. McNair , Washington, D.C. The symposium brought together a diverse mix of more than 230 participants from maritime companies, associations, operations and fusion centers, navies, coast guards and government agencies from around the world.

GMISS is sponsored in conjunction with the U.S. Maritime Administration (MARAD) and under the auspices of the U.S. National Maritime Domain Awareness (MDA) Stakeholder Board which report to the Maritime Security Interagency Policy Committee of National Security Council. It is dedicated to enhancing the information sharing relationships between the maritime industry and government through the coordination of the Office of Global Maritime Situational Awareness (OGMSA).

Background

A Need for New Approaches

OGMSA was created based on the understanding that there are significant benefits to be gained through an increase in the level of open exchange of non-classified maritime information (*please see Appendix A for more information on OGMSA*). As witnessed within other industries (airline, trucking, manufacturing, etc.), an increase in the open exchange of maritime information can improve the maritime industry's efficiency, together with its safety and security, and the environment within which it operates.

Within each of the United States' guiding documents and initiatives calling for greater global maritime security, such as the National Strategy for Maritime Security and the "Cooperative Strategy for 21st Century Sea Power," are such core concepts of openness as maximizing the share-ability of maritime data, multilateral versus bi-lateral data sharing, growing both long term interagency and international partnership trust, and collaborating with the maritime industry. When such concepts are acted upon while embracing a broader rationale for information sharing, such as commercial efficiency, maritime safety, and environmental management, the result is greater transparency in maritime affairs to the benefit of all. By sharing maritime data that benefits a broader range of potential contributors, a more complete picture of the entire maritime domain becomes available to support maritime security.

Key to this shift to openness is greater cooperation with the industry that operates throughout the domain, and a broadening of the dialog along non-traditional lines of communication and engagement.

The U.S. Coast Guard Cutter USCGC Thetis (WMEC 910) sails in formation with maritime forces from Argentina, Brazil, Canada, Chile, Colombia, Ecuador, Germany, Mexico, Peru, U.S. and Uruguay off the coast of Florida during Exercise UNITAS Gold. (U.S. Coast Guard photo by Petty Officer Seth Johnson)

Need for Conference Coordination

The realization of this fact spawned a surge in energy to expand industry outreach. However, it needed focus. By informal count, there were well over 20 commercial outreach meetings sponsored by U.S. government entities in Fiscal Year 2008. The plethora of conferences and symposiums, all purporting to enhance communications and information sharing between government agencies and the maritime industry, created the following list of complaints from industry and government:

- Too many conferences that say the same thing; objectives are the same.
- Too many conferences with no follow through.
- Too many one-way conversations (government talks, industry listens).
- Too many conferences that establish working groups but no usable products are created.
- Conference results are not shared across agencies, nor is there an attempt to build on issues raised.
- Too many duplicative information requests by the U.S. government and international organizations.
- Too many unilateral demands on the industry.

These issues have created frustration on the part of commercial entities whose very survival depends on containing costs, while providing very little headway in information sharing. In sum, the static of U.S. government commercial outreach drowned out the intended dialog and actions.

CBP officers take a moment to discuss strategies for searching arriving cargo. (U.S. CBP photo by James R. Tourtellotte)

Need for a Forum Free from Fear of Retribution

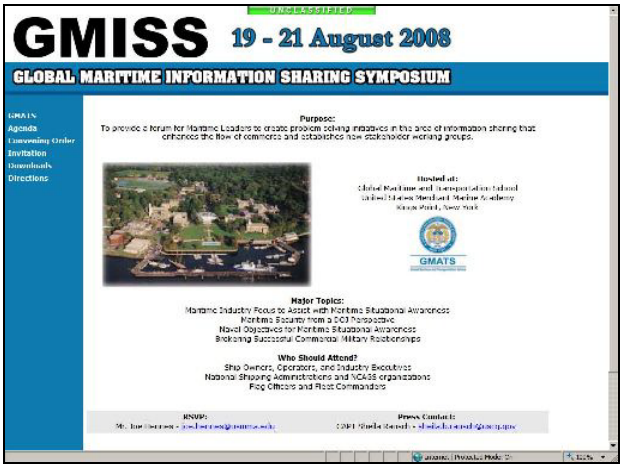
There have been a wide range of productive outreach efforts at the federal, state, and local levels. However, the majority of these initiatives have been undertaken by agencies with a regulatory relationship with the industry. Any dialog conducted in such fora may be inherently inhibited by the regulatory basis of these relationships which in turn may prevent the acceptance by all parties of what could be mutually beneficial best practices. Leveraging best practices and establishing the trust required to move to open sharing of maritime information profits from the involvement of an honest-broker with no regulatory authority whose unbiased intent is to maximize the benefit to all parties.

Need for Broader Industry Representation

Within U.S. government circles, a reference to the maritime industry remains too frequently a reference to its ship owners, or at the outside, its cargo interests. The industry however, is much deeper and broader in its equities. The influence and information from maritime charterers, underwriters, brokers, ship agents, private equity, mortgage holders, mariners' associations, vendors, and the seafarers themselves, presents a whole new layer of capability whose information, while routinely exchanged to the benefit of industry, remains untapped by most involved in government MDA. To not involve this layer of interests is to remain oblivious to the forces which keep global maritime trade moving forward and the wealth of maritime information they can share. These crucial maritime interests and viewpoints need to be equally involved in any changes to their industry if MDA is to benefit from their partnership.

(Maersk Line photo)

Original Conference Intent



Based in part on the above OGMSA observations, the Global Maritime Information Sharing Symposium was created as a venue to enhance communication and maritime information sharing between government and the maritime industry. It brings together and coordinates government entities that play a role in maritime commerce in a more cohesive outreach to industry. A guiding principal is that an effective partnership with industry can only be established if the needs and concerns of industry are understood and considered. Specifically, GMISS seeks to remove inhibitors to efficient commerce through more effective information sharing. In other words, how can we collectively enhance safety, security, and environmental management without unduly hampering commerce? More to the point, can we provide value for industry for every request for their information?

The overall objectives of GMISS are to:

1) Harness the growing energy for conferences and commercial outreach initiatives across the government. Specifically, identify priorities among those information sharing issues that are emerging from government-commercial relations and ensure resources are available to work them.

2) Create a systematic, annual cycle of coordination that ensures the identification of and engagement in government-industry information sharing issues. GMISS will be the annual meeting to assess what has been accomplished over the last year and ensure priorities are clear for the coming fiscal year.

3) Provide a forum for stakeholders in government and the global maritime industry to address issues and initiatives central to information sharing needs that enhance maritime situational awareness in an environment free of fear or coersion.

GMISS was specifically designed to:

- Provide synergy of efforts, husbanding of resources, and coordinated outreach across all MDA stakeholders.
- Leverage information sharing accomplishment by the Departments of Homeland Security (DHS), Transportation (DOT), Defense (DOD), Justice (DOJ), and State (DOS), industry, state and local law enforcement agencies, and maritime organizations worldwide.
- Present a single U.S. government face to the industry and help resolve their MDA concerns and issues
- Exchange best practices
- Create more trust and comfort for information sharing by industry and government

The long range (multi-year) objectives of the GMISS include:

- Coordinate the U.S. government's commercial outreach across all MDA stakeholders to ensure a more unified path for addressing industries issues/concerns and innovations.
- Implement industry/government working groups to provide a venue for maritime leaders to create problem-solving initiatives in the area of information sharing that enhance maritime security and the flow of commerce, and establish new stakeholder working relationships.
- Identify and act on opportunities that strengthen Information Sharing processes and agreements.
- Promote regional involvement.
- Engage the range of stakeholders needed to properly achieve effective maritime awareness.

Related Efforts

The Director Global Maritime and Air Intelligence Integration (GMAII) conducted a one-day "Protecting the Global Supply Chain Conference" in June 2008 as part of a series of workshops initiated by the Office of the Director of National Intelligence (ODNI) and two private sector partners: the U.S. Chamber of Commerce and the Intelligence and National Security Alliance (INSA). The purpose of the workshop was to exchange views and perspectives on issues of common interest and concern to the private sector, U.S. government and the Intelligence Community. (*please see the GMISS 2008 Summary Report, Tab 5 at www.gmsa.gov/gmiss for the full report*).

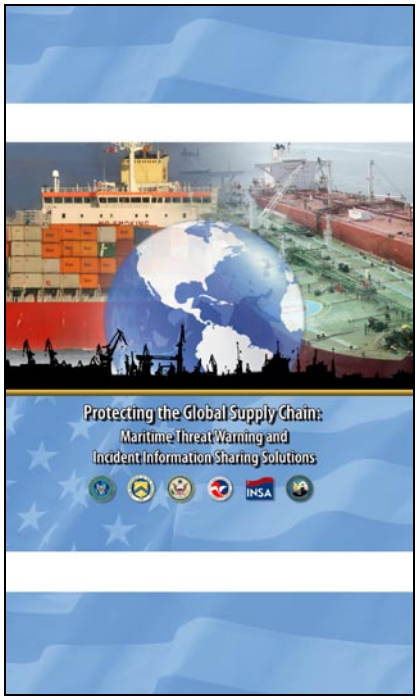
Ms. Wendy Walsh, Homeland Defense and Security Coordinator at the U.S. Naval Postgraduate School, facilitates a collaborative session at MIST LA-Long Beach.

On August 20 and 21, 2008, the U.S. Maritime Administration and Naval Postgraduate School conducted their first symposium under the Maritime Information Sharing Taskforce in the ports of Los Angeles and Long Beach, coincidentally, on the same days OGMSA conducted GMISS 2008 in King's Point, NY (p*lease visit www.gmsa.gov/gmiss to read the full report*).

On September 17 and 18, 2008, the Navy's Maritime Liaison Unit – Latin America (MARLU-LATAM) conducted a Maritime Security Conference in Miami, FL that launched the unit's industry outreach efforts.

In view of the above related efforts, in developing the GMISS 2008 Summary report (*please see Appendix H for an executive summary, or visit www.gmsa.gov/gmiss to read the full report*), OGMSA also pooled the findings of the Global Supply Chain Workshop, MIST, the Maritime Security Conference, and other maritime awareness/information sharing research efforts and workshops. This fusion of information produced more robust and more nuanced findings than could otherwise have been generated by the discussion at GMISS 2008 alone. It also allowed the consolidated findings to serve as the foundation for development of GMISS 2009 Agenda.

Going forward, OGMSA and GMAII partnered for their 2009 commercial outreach efforts, merging the Protecting the Global Supply Chain Conference with GMISS. The Office of the Director of National Intelligence played an integral role in planning and executing GMISS 2009.



OGMSA and GMAII participated in the second MIST symposium, conducted in Seattle, WA. Prior to developing its research objectives for Puget Sound, the Naval Postgraduate School worked with OGMSA to align the desired outcomes of MIST and GMISS, and topics planned for discussion at GMISS were introduced at MIST Puget Sound. The results of MIST were integral to developing GMISS 2009.

OGMSA and MARLU-LATAM also coordinated efforts in developing the MARLU's 2009 Conference topics and GMISS 2009 to ensure each produced their own unique value and were not redundant efforts on the part of industry attendees.

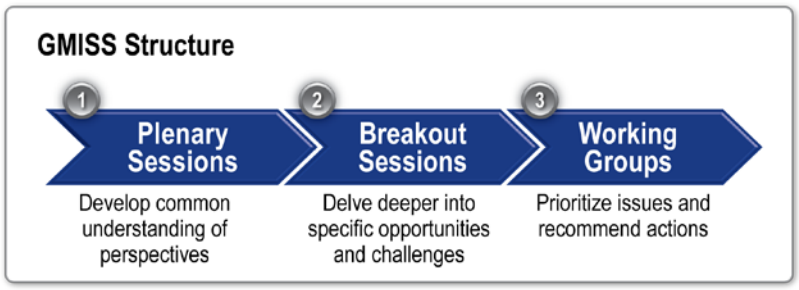
OGMSA's future efforts will be coordinated with, while not hampering, these parallel conferences.

Ongoing Support

During 2009, the U.S. Maritime Administration created a complete program centered on GMISS that also supports the ongoing GMISS working groups and the Naval Postgraduate School's Maritime Information Sharing Taskforce (MIST). For the first time, seed funding has been budgeted for GMISS beginning in Fiscal Year 2010. In addition, in the wake of GMISS 2009, OGMSA received invitations from organizations worldwide to partner with them to conduct GMISS 2010 in their areas of operations. Several organizations have also contacted OGMSA to discuss their further involvement in GMISS 2010 rather than conducting their own separated conferences or symposia.

GMISS Structure

GMISS is based on an "issue-to-working-group" progression. In plenary sessions, experts from throughout the maritime domain present their perspectives to give participants a shared framework for understanding key issues. In breakout sessions, participants delve deeper into the issues that most concern them, again benefitting from the perspectives of a sampling of maritime speakers. Finally, GMISS participants form into working groups to clarify the issues, to prioritize them for action in the coming year, and to recommend possible optimal courses of action. These working groups continue to function throughout the year, ensuring the recommended actions benefit from ongoing input from the members of the maritime community with the appropriate knowledge and experience, and a stake in the outcome, and report back at the next GMISS event.



GMISS – MIST Partnership

The intent of MIST is to integrate local private sector perspectives into a national picture for the sharing of maritime threat information. Its role is to facilitate the interaction between government and the private sector and focus on delivering actionable recommendations based on private-sector input. The taskforce strives to capture the voice of the private sector maritime industry at the local/regional port level in a way that will:

- capture best practices in information sharing
- create a structure for collaborative problem solving
- convey unique local issues to national policy makers

An Interagency Approach

The MIST team is led by the Maritime Defense and Security Research Program (MDSRP) at the Naval Postgraduate School (NPS) in coordination with the U.S. Maritime Administration. Significant funding is provided by the Assistant Secretary of Defense for Homeland Defense. Conceived as a multi-agency process, MIST coordinates with a number of private and public agencies:

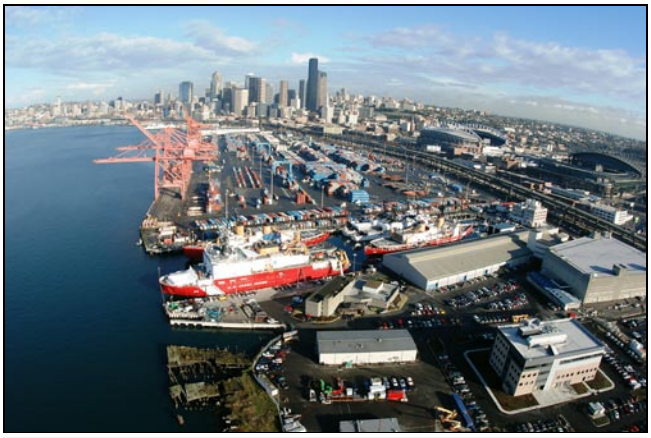
- The U.S. Coast Guard
- U.S. Customs & Border Protection (CBP)
- The Office of Global Maritime Situational Awareness (OGMSA)
- The Director of Global Maritime & Air Intelligence Integration (GMAII)

- The Marine Exchanges
- The Pacific Maritime Association
- Port Authorities
- Local and State Responders

The Regional Perspective

In 2008, the MIST Steering Committee created an exploratory process for facilitating the sharing of threat information. This process began with an event at the Port of Long Beach/Los Angeles that included a local workshop and a social networking web site. Continuing in Seattle in 2009, event activities expanded to include a study of local information flow and additional community building (*please see Appendix I*). Future plans include a mapping of local networks and a mechanism for consolidating national feedback. A MIST symposium in the Port of Honolulu followed GMISS in October 2009.

GMISS and MIST are now conducted in close cooperation to maintain a unified government voice for industry outreach while developing a well-rounded understanding of the industry perspective. While GMISS focuses on the national and international level, MIST reaches out at the local and regional level, ensuring local concerns and issues are understand and addressed.



The port of Seattle, Washington
(USCG photo by Petty Officer 3rd Class Tara Molle)

To ensure that OGMSA's national/global efforts align with local/regional work efforts, both organizations look at incentives and models for information sharing and ways to streamline government requests. The MIST team probes for operational-level goals, gaps, barriers and risks in the sharing of threat information. They conduct ongoing research and meet with local port personnel for feedback on specific policies and technologies. GMISS applies this research in ongoing working groups comprised of government and industry representatives to develop innovative strategies, and brings the industry voice to bodies that coordinate national-level maritime security policy.

This partnership ensures decisions reached at the highest levels actually make sense in day-to-day operations of ports around the country.

GMISS 2009

OGMSA coordinated every detail of GMISS 2009, including transportation, lodging, staffing, catering, and facilities, thus guaranteeing all attendees the ability to participate to the fullest extent possible in addressing substantive maritime issues during the three day conference.

Several federal agencies partnered with OGMSA to present GMISS 2009, providing valuable resources and lending their specific areas of expertise:

- The U.S. Maritime Administration (MARAD) (Department of Transportation)
- The U.S. Coast Guard (Department of Homeland Security)
- The Office of Community Oriented Policing Service (COPS) (Department of Justice)
- U.S. Fleet Forces Command (USFF)
- Naval Cooperation and Guidance for Shipping (NCAGS)
- The Naval Postgraduate School (NPS)
- The Office of the Director of National Intelligence (ODNI)
- The National Maritime Intelligence Center (NMIC)

The National Defense University in Washington, D.C. made its state-of-the-art facilities available and provided invaluable logistics, information technology, and audio-visual support without which the symposium would not have been possible.

In addition, Marine Log Magazine rolled its 2009 Combating Piracy conference into GMISS 2009. While GMISS is intended to create more effective maritime information sharing independent of any specific mission or application, no meeting between government and the maritime industry could progress far in 2009 without the topic of piracy moving repeatedly to center stage. Therefore, OGMSA positioned piracy as a useful framework for examining larger-picture challenges, successes, and opportunities during GMISS 2009.

In addition, GMISS 2009 benefited from the expertise of an amazing array of participants, which included ship owners and operators, shipping brokers and agents, vessel underwriters, maritime educators and associations, maritime information venders, U.S. federal, state, and local officials from municipal police officers to deputy cabinet secretaries, and partners from navies, coast guards, maritime administrations and maritime operations centers around the world.

GMISS 2009 was held at Lincoln Hall on the National Defense University, Washington, D.C.

This combination of vantage points was focused in four working groups, each addressing a specific issue.

- Working Group A: Building a Global Maritime Information Exchange Grid – Is it Possible?
- Working Group B: Bridging the Understanding Gap Between Maritime Industry and Government
- Working Group C: Resolving Information Privacy, Proprietary & Classification Concerns
- Working Group D: Piracy - A Model of Co-developed, Mutually Beneficial Policies?

GMISS 2009 used a Web-based collaboration software application to ensure attendees were able to accurately and anonymously record their input during every stage of the symposium. This was particularly valuable during working groups and breakout sessions. It promoted broader participation, and enabled attendees to consistently build on points developed throughout the three-day symposium.

To ensure all participants could share their opinions, experience, and expertise without fear of reprisal, the symposium was conducted under the Chatham House Rule.[1]

A summary of GMISS 2009 proceedings and results are presented in the following section. For more in-depth reporting of the presentations and deliberations of GMISS 2009, please see Appendix D.

NOTE: Appendix D contains summarized excerpts of individual presentations and follow-on discussions as transcribed at GMISS 2009 by OGMSA team members. It is not intended to represent all that was stated, presented or discussed nor to indicate that inclusion or exclusion of a specific concept or statement represents the speaker's position or priorities. Summarized excerpts as transcribed by OGMSA are combined with participant comments as entered by the participants during GMISS 2009, into the collaborative software. These comments may not accurately reflect was being stated, presented or discussed.

These summary excerpts and comments are being provided for general discussion and should in no way reflect on the speakers or any individual participant.

1 "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed" Chatham House, http://www.chathamhouse.org.uk/about/chathamhouserule/

2 National Security Presidential Directive NSPD-41, Homeland Security Presidential Directive HSPD-13, Dec. 21, 2004

II. Summary of Proceedings

Recurring Themes

Several themes emerged during the plenary sessions, panels and breakout sessions of GMISS 2009. Because the range of presenters was selected to provide a broad cross section of the global maritime community of interest, the frequency of the introduction of these themes by both presenters and participants suggests the existence of a general consensus as to priorities among the community. For a matrix of recurring themes and their frequency of occurrence, please see Appendix F.

Coordination/Information Flow

Issues concerning the coordination of MDA were raised more often than any other (24 instances over two days). Chief among coordination concerns was a desire for clearer leadership in MDA. These ranged from the repeated industry query of "Who's in charge of MDA?" to a desire for at least a single coordinating office in the federal government. Meanwhile, at least one government representative sought a focal point for industry on the waterfront. The Deputy Secretary of Transportation cited his experience at the state government level during 9/11 to demonstrate the value of effective coordination between federal, state, and private sector during emergencies, calling the state's relationship with Coast Guard and industry one of the greatest strengths he was able to tap in the aftermath of 9/11. The Department of Justice, which brought a high level of expertise in information sharing to the symposium, pointed out the need for better coordination with private security providers. The Department of State sought feedback to improve OSAC coordination with industry, which was repeatedly identified by industry representatives as a model for best practices, suggesting a correlation between continuous improvement in coordination and success. A better understanding of how to improve coordination among navies and governments was also requested. The complex web of regulations at various levels of government was introduced repeatedly. One representative of a maritime association pointed out that if government did coordinate industry information so it received all the information it desires, the government would be overwhelmed with data. The emergence of U.S. maritime spatial planning under the Obama Administration was identified as an additional layer of complexity that must be addressed and coordinated. A member of the intelligence community urged that industry be included now in government MDA architecture planning to ensure effective policies by both government and industry.

View from the bridge of a tanker entering Puget Sound (USCG photo)

The flow of information between industry and government was the second most common topic of discussion (16 instances). Speakers from government agencies around the world stressed government's need for information from the maritime industry to accomplish a wide range of missions, such as national security and prosecution of pirates. Industry attendees made it clear that large amounts of information were available which could paint a fairly complete picture of shipping. However, government and industry participants also repeatedly raised the requirement for a better understanding of what information was needed and clarification of how to provide it to government. More than once, industry representatives explained that they don't necessarily need to know the actual intelligence information, but how to guard against or look out the possible threat, including how to best deploy resources based on current threats. A need was also expressed from inside industry for maritime companies to improve their own maritime awareness to their own benefit.

Mutual Understanding

Another related theme that emerged was the need for improved government understanding of industry and industry understanding of government. In addition to being the focus of a working group on Day Three, the topic surfaced eight times during the first two days of the symposium. There was general agreement that improved mutual understanding was essential before effective MDA could be achieved.

A container ship works with the Coast Guard during exercises aimed at preventing proliferation of weapons of mass destruction. (USCG photo by PA3 Stacey Pardini)

Classification

On ten occasions during the plenary, panel, and breakout sessions, concerns were expressed about the impact of classification on government/industry information sharing. Most commonly, the need to reduce classification was raised. Related challenges, recommendations and successes were also offered. A perceived trend in government to move MDA programs into intelligence offices raised concerns of moving backward regarding classification.

Models for Success

Several presenters and participants initiated discussion regarding models for success in MDA (8 instances). These included:

- A matrix indicating who leads sharing of which types of data
- Need for confidence building, simple cost structure, inclusive approach
- Equal partnerships in which every participant has a say
- Start with bilateral linkages first and expand to multilateral later
- Start with closest neighbors, then expand
- Build on previous successes, such as anti-drug initiatives
- Empower participants at all levels to contribute as early as possible, following the example of the Amber Alert system.

GMISS

The symposium itself was the topic of several discussions (8 instances). For the most part, GMISS was seen as a positive development and an effective tool for improving industry/government information sharing. It was pointed out that symposium discussion must translate into actionable projects that can be tracked and accomplished. It also surfaced that GMISS objectives are being adopted by other initiatives. However, participants also pointed out flaws in the present roster of participants, identifying several organizations that must become involved for GMISS to succeed, including the International Maritime Organization (IMO), the Port Management Association of Eastern and Southern Africa (PMAESA), the Organization of American States (OAS), the European Union (EU), World Customs Organization (WCO), the South Asia Regional Port Security Cooperative (SAARPSCO), and the Maritime Liaison Office (MARLO).

Immediate Information vs. Vetted Information

During the first panel discussion on the first day, an extended discussion emerged regarding the merits of immediate information as opposed to vetted information. It became clear that both are valuable in turn. Introducing small amounts of reliable information as quickly as possible enables participants throughout the community to begin focusing on an issue and contribute both information and analysis from all levels. This was viewed by industry participants as significantly preferable to waiting until an entire vetted report could be released. The rapid expansion of awareness that rapid sharing can provide was strongly endorsed. However, the need for the information that is released by government to be trustworthy was viewed almost uniformly as essential. Industry participants also noted that they do not necessarily need to know what the intelligence is; if they are confident the guidance is trustworthy, they may only need recommendations that guide allocation of resources and an awareness of what types of threats to prepare for.

Anti-Piracy Capacity

Piracy discussions emerged throughout the symposium, as was anticipated. On several occasions outside the piracy working group the discussion centered on information sharing as it related to piracy. Three high-level U.S. government officials stated the need for more information to counter piracy (5 instances). A well-respected industry representative added that the global legal system was failing to prosecute pirates; a situation an Assistant Secretary of State indicated could be improved with better information sharing. LRIT was identified as necessary despite the universal adoption of AIS because, while AIS is often disabled to avoid detection by pirates, LRIT may allow ships under attack to continue transmitting their location of maritime security forces.

TWIC Implementation

(USCG illustration by Petty Officer 1st Class NyxoLyno Cangemi)

Implementation of the TWIC program was raised on three separate occasions, with general agreement that it has been challenging. Improved sharing of information was requested insofar as TWIC could be universally recognized as valid identification, particularly across the Transportation Security Administration.

MDA Silos

On three occasions concern was expressed that some efforts to develop MDA are creating new silos rather than moving information out of silos.

Civil Liberties

The issue of civil liberties was raised three times during the plenary, panel, and breakout sessions. Notably, in all three instances, the need to safeguard civil liberties in the face of increased information sharing was brought up by federal government representatives: specifically, members of the intelligence community.

Working Group Results

GMISS working groups met for the majority of the third day of the symposium, each addressing a unique aspect of maritime information sharing:

- Working Group A: Building a Global Maritime Information Exchange Grid; Is it Possible?
- Working Group B: Bridging the Understanding Gap between Maritime Industry and Government
- Working Group C: Resolving Information Privacy, Proprietary & Classification Concerns
- Working Group D: Piracy - A Model of Co-developed, Mutually Beneficial Policies?

After extensive deliberations, each group reported back to the entire symposium, including Points of Discovery, Actionable Items, and Ongoing Discussion Points/Recommendations.

The deliberations and results are included in Appendix D of this report in abbreviated form to ensure confidentiality for individual participants. Results are also summarized in matrices in Appendix G. Due to the specific nature of this year's working group topics, there was little overlap in findings among working groups. However, groups reported a few shared results, as summarized below.

Points of Discovery

Both Working Group B and Working Group D found that government and the maritime industry need to significantly improve mutual understanding: a concept that surfaced repeatedly throughout the symposium.

Working Groups C and D both identified a need for a single coordinating point of contact to assemble classified and non-classified information from industry and government each, and to push it out in usable form one to the other.

The need for an international maritime governance structure with clear objectives and goals emerged in both Working Group A and Working Group D.

Additional key points of discovery that arose in individual working groups concerned the need for representation of industry, government, and NGOs in the majority of maritime information sharing discussions; the need to identify specific requirements for global maritime information sharing; and identification of specific strengths and weaknesses of the global collaboration model developing to counter piracy.

Actionable Items

Two shared actionable items can be gleaned from among the four working groups.

Both Working Group A and Working Group C essentially recommended development of a network to link existing information sharing infrastructure and consolidate AIS sharing networks.

Working Groups B and D recommend evaluating existing training to improve mutual understanding, identifying gaps, and instituting the needed additional training.

Several additional actionable items were somewhat related to each other, involving:

- Global MDA governance
- Single point of contact for crises
- Specific actions to build a global maritime information sharing grid
- Building on successes
- Greater access to U.S. government policymakers
- Global marketing of maritime information sharing

Ongoing Discussion Points and Recommendations

None of the recommendations for further discussion were shared among working groups. These specifically addressed finer points of the topics each group addressed.

GMISS participants prioritize key information sharing issues in a working group. (OGMSA photo)

Shared Priorities Inferred from GMISS Working Groups

By combining shared elements from these three sets of information, OGMSA has inferred possible courses of action which may meet the shared intents and priorities of the working groups. They are as follow.

Global Grid and Governance

Identify and empower a non-governmental organization – with industry, government, and NGO representation – to provide non-binding information sharing dispute resolution between conflicting interests, and to lead:

- development of a global maritime information sharing grid
- establishment of information sharing standards
- consolidation of existing systems
- linking of existing sites and networks.

(Working Groups A, B, C and D)

Single Point of Contact for Policy

Identify a single trusted point of contact (policy vice operational) to coordinate maritime awareness/MDA development issues between the U.S. government and the maritime industry.

(Working Groups A, C, and D)

Single Point of Contact for Information Flow

Identify a single trusted point of contact (operational vice policy) to manage and coordinate ongoing information flow between the maritime industry and the U.S. government, including tip reporting, collaborative awareness and intelligence development, threat warnings, and other alerts.

(Working Groups B, C, and D)

Close Gaps in Understanding

Assess current mechanisms for developing mutual understanding between industry and government, promote these opportunities to all members of the GMCOI, and develop a plan to fill the gaps left by the existing opportunities.

(Working Groups B, C, and D)

Link Regional Centers into a Global Structure

Identify or establish regional centers to manage ongoing information flow among all stakeholders in their areas of operations; form a board comprised of these regional entities to coordinate global flow of

maritime information under an international maritime information sharing governance structure with clear objectives and goals.

(Working Groups A, C and D)

Implementation

These possible courses of action will be presented to the four ongoing GMISS working groups for consideration and refinement in order to develop a set of specific actions on which the groups can collaborate. In addition, each working group will address its own specific action items. OGMSA will provide coordination between working groups to ensure efforts complement each other.

All GMISS participants are welcome to continue their participation through the ongoing working group or groups of their choosing.

III. Ongoing Working Groups

The four working groups developed during GMISS 2009 will continue to address the issues they discussed at the symposium, and pursue their recommended courses of action. OGMSA will be using the same Web-based collaboration software employed during the symposium for some of this effort. In addition, blogs have been established for the overall GMISS effort and for each working group. All members of the Global Maritime Community of Interest are invited to join these ongoing conversations at www.GMISSonline.blogspot.com.

The four working groups will be proceeding as follows:

GMISS discussions continue at www.GMISSonline.blogspot.com

GMISS Working Group A: The Information Grid Working Group

Building a Global Maritime Information Exchange Grid

Primary Goal:

Connect maritime operations centers, fusion centers, maritime exchanges, government maritime information hubs, etc. into a global maritime information exchange grid that includes easy mariner access to provide and receive information.

Blog:

www.gmissInformationGrid.blogspot.com

Coordinator:

CAPT Ralph Nieves, USN
Chief, Data Sharing and Infrastructure Branch
Office of Global Maritime Situational Awareness
Email: Rafael.F.Nieves@uscg.mil
Voice: 202-372-3062
Fax: 202-372-3905

Actionable Items for 2009:

- Define the "as is" state of the global grid: what is useable, discoverable, accessible
  - information sharing sites
  - exercises
  - collaborations
  - laws & polices
  - best practices
- Develop a meta site of maritime information exchanges
- Create a panel to define the essential elements of information for the maritime global community
- Develop and implement a marketing plan for government / industry / NGO maritime information sharing

GMISS Working Group B: The Understanding Gap Working Group

Bridging the Understanding Gap between the Maritime Industry and Government

Primary Goal:

Enable members of industry to understand how government makes and enforces the policies that impact them, and enable members of government to understand how government policy impacts industry.

Blog:

www.gmissUnderstandingGap.blogspot.com

Coordinator:

CDR Jim Feldkamp, USN
Chief, Outreach and Coordination Branch
Office of Global Maritime Situational Awareness

Email: James.L.Feldkamp@uscg.mil
Voice: 202-372-3081
Fax: 202-372-3905

Actionable Items for 2009:

- Research the environment and evaluate training and internships currently available within the maritime industry.
  - (This training must be unclassified and examine existing inter-agency, inter-government, inter-industry training to establish a baseline for future programs.)
- Determine what is still needed.
- Establish industry participation on the Maritime Domain Awareness Stakeholder Board.
- Establish industry participate (by invitation) on Maritime Security Inter-Agency Policy Committee of the National Security Council

GMISS Working Group C: The Information Safeguards Working Group

Resolving Information Privacy, Proprietary & Classification Concerns

Primary Goal:

Identify specific barriers to information sharing based on privacy, proprietary and classification concerns, and develop a resolution that preserves civil liberties, commercial competition, and national security.

Blog:

www.gmissInformationSafeguards.blogspot.com/

Coordinator:

CAPT Dave Sanders, JAGC, USN
Legal Counsel
Office of Global Maritime Situational Awareness
Email: David.F.Sanders@uscg.mil
Voice: 202-372-3063
Fax: 202-372-3905

Actionable Items for 2009:

- Develop a pilot program utilizing existing infrastructure to disseminate information. (for example, DOD's Joint Integration of MDA program & the Maritime Information Sharing Taskforce)

- Expand the America's Waterway Watch program to encompass all users. For example, where does a commercial ship call? When the call is received, is the operator trained to deal with the information?
- Consolidate regional proliferation and global consolidation of AIS data
- Examine the use of a non-government organization to manage international governance options for global AIS sharing
- Establish a uniform U.S. government policy mandating interagency information sharing
- Develop an information sharing dispute resolution procedure
- Develop training for information sharing professionals; transform the culture of "need to know" to "need to share"

GMISS Working Group D: Operational Collaboration Model Working Group

Building on Anti-Piracy as a Model of Co-Developed, Mutually Beneficial Policies

Goal:

Develop an optimum model of operational collaboration between industry, navies, coast guards and other maritime security entities that is scalable and applicable to maritime threats and crises worldwide.

Blog:

www.gmissCollaborationModel.blogspot.com/

Coordinator:

CAPT Dale Ferriere, USCG
Chief, Plans and Policy Branch
Office of Global Maritime Situational Awareness
Email: Dale.V.Ferriere@uscg.mil
Voice: 202-372-3058
Fax: 202-372-3905

Actionable Items for 2009:

- Establish a single point of contact for all information flow, including reporting by industry and the dissemination of information to industry.
- Develop a single point of contact for maritime crises.
- Identify and develop the best course of action to educate government personnel that impact the maritime industry on industry commercial fundamentals.

- Build on the response models created by United Kingdom Maritime Trade Operations (UKMTO) Office and the Shared Awareness and Deconfliction (SHADE) group.
- Ensure maritime security best practices and successes are shared in a common environment to drive future development industry standards, such as the inclusion of ship defensive measure in future ship design.
- Regularly record and review lessons learned to maintain coordination between industry and government developed thus far and preserve confidence in communication.

Return to Action

The GMISS ongoing working groups are scheduled to resume operation in January 2010. Members of the Global Maritime Community of Interest who are willing to lend a hand with these efforts are invited to contact working group coordinators directly.

IV. Appendices

A. OGMSA Background

B. Maritime Domain Awareness Enterprise Hubs

C. GMISS 2009 Agenda

D. GMISS 2009 Presentations

E. Recurring Themes during GMISS Sessions

F. GMISS Working Group Common Conclusions

G. GMISS 2008 Executive Summary

H. 2009 MIST (Puget Sound) Executive Summary

Appendix A
OGMSA Background

Excerpted from the OGMSA Annual Report 2009

In 2004, the U.S. federal government initiated actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests[2]. National Security Presidential Directive NSPC41/Homeland Security Presidential Directive HSPC13 established the nation's first national maritime security policy December 2004. Under that policy, and the supporting strategies, plans, and concept of operations *(Please see Exhibit 1, page 10)*, the Office of Global Maritime Situational Awareness (OGMSA) was established in August, 2007.

A foundational concept in U.S. maritime security policy is Maritime Domain Awareness (MDA). MDA is the effective understanding of anything associated with the global maritime domain[3] that could impact the safety, security, economy, or environment of the United States[4]. Under the U.S. maritime security strategy, MDA is a key national security requirement, it is heavily dependent on information sharing, and requires unprecedented cooperation among the public and private sectors, both nationally and internationally.[5] It is achieved by coupling awareness of activity within the maritime domain with knowledge of intent or threat information[6].

OGMSA is a multi-agency office that coordinates efforts among U.S. federal, state, and local agencies, tribal authorities, other nations, and the maritime industry to achieve the situational awareness aspect of MDA in support of the U.S. National Plan to Achieve Maritime Domain Awareness (NPAMDA)[7]. Because OGMSA does not reside within any specific agency and is chartered to develop global MDA independent of any specific mission or usage, it is recognized as an honest broker on behalf of the interests of all members of the global maritime community of interest in developing effective MDA.

The Maritime Security Interagency Policy Committee (MSIPC) is the primary forum for coordinating and implementing the U.S. National Plan to Achieve MDA.[8] The MSIPC operates within the framework of the National Security Council (NSC) and reports via the NSC Deputies Committee and Principals Committee to the President of the United States. OGMSA reports to the MSIPC, of which the Director of OGMSA is a member, and is responsible, through the National MDA Stakeholders Board and its Executive Steering Committee, for administering the National Plan to Achieve MDA (NPAMDA). Reporting includes participation in quarterly meetings as a member of the MSIPC, and an annual report to the MSIPC on OGMSA's activities and implementation of MDA directives. The intent of this report is to fulfill that reporting requirement.

In addition, the Director of OGMSA has dual reporting responsibility to the Commandant of the U.S. Coast Guard and to the U.S. Chief of Naval Operations, and keeps each apprised of MDA progress and OGMSA activities through regular meetings and briefings either directly, or through their respective staffs.

(To read the entire report, please visit www.gmsa.gov)

---

2 National Security Presidential Directive NSPD-41, Homeland Security Presidential Directive HSPD-13, Dec. 21, 2004

3 NSPD-41/HSPD-13 defines the maritime domain as: "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."

4 NSPD-41/ HSPD-13, Dec. 21, 2004

5 National Strategy for Maritime Security (NSMS), Sept. 2005

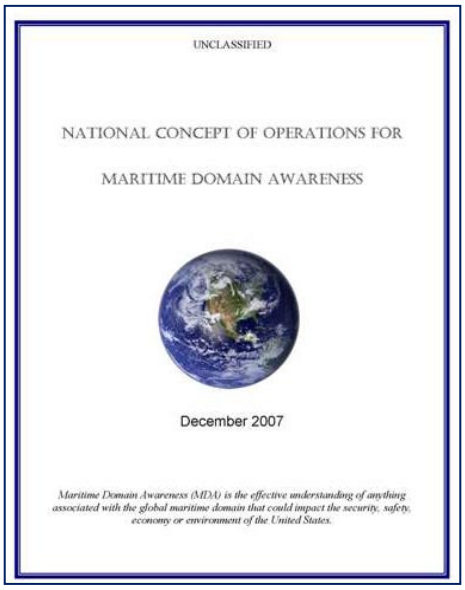
6 National MDA Study Interagency Investment Strategy (IAIS), May 3, 2007

7 National Concept of Operations for Maritime Domain Awareness, (MDA CONOPS), Aug. 2007

8 National Plan to Achieve Maritime Domain Awareness (NPAMDA), Oct. 2005

Appendix B
Maritime Domain Awareness Enterprise Hubs

Paraphrased from the U.S. National Concept of Operations for Maritime Domain Awareness


UNCLASSIFIED

NATIONAL CONCEPT OF OPERATIONS FOR

MARITIME DOMAIN AWARENESS

December 2007

Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy or environment of the United States.

Current technical, cultural, political, and policy limitations inhibit day-to-day attainment of MDA. The National MDA CONOPS proposes the establishment of Enterprise Hubs based on the "pillars" of MDA – vessel, cargo, people and infrastructure information – and a fifth Enterprise Hub to develop the architecture for connecting the data digitally. They are located at existing agencies with representation from other members of the Global Maritime Community of Interest (GMCOI) as needed. These Hubs will be the lead coordinators for their MDA pillar and facilitate sharing information and intelligence among the GMCOI.

Designation as an Enterprise Hub confers two primary responsibilities; overall coordination of information flow for the respective subject area both domestically and internationally, and facilitating the sharing of related intelligence, information, and data. Enterprise Hubs are intended to leverage their experience and expertise to provide leadership for the community in a particular area, not to be the exclusive federal provider of information and products for that subject area. The near-term concept calls for MDA Enterprise Hubs for the four MDA pillars, as well as architecture.

These Enterprise Hubs need to be linked to intelligence and information providers and be able to share pertinent data with the GMCOI. Each Enterprise Hub will receive intelligence, information, and warnings generated by the GMCOI, and each Hub will make available global maritime situational awareness data and information to appropriate decision-makers and global maritime intelligence partners. Current political, cultural and fiscal limitations to the implementation of viable technologies dictate a regional or local approach to analysis, fusion, and dissemination. In the near-term, the analysis and fusion of intelligence and information regarding the MDA pillars will be performed by those local, regional, and national entities that currently perform an analysis function. Although a department or agency may be designated an Enterprise Hub lead, this designation, in and of itself, does not give it an analysis function. However, that same department or agency may, as part of its mission set, possess an analytical capability. In the future, coordination will be largely virtual, with all MDA users networked by a multi-level security, services-oriented architecture. There may also be a need for additional Hubs in the future to address areas such as finance, ownership, and international and regional issues.

While agencies that host Enterprise Hubs perform collection, fusion and analysis consistent with their current roles and responsibilities, these functions compliment the primary objective of a Hub. The Enterprise Hubs are sources of subject matter expertise for the directors of the Office of Global Maritime Situational Awareness and Global Maritime and Air Intelligence Integration, administered by the Director of OGMSA.

MDA Enterprise Hubs:

- lead interagency information coordination for their respective pillar of MDA information;
- facilitate the sharing of intelligence, information and data;

- inventory and catalog the databases and information sources that contribute to achieving MDA, serve end user requirements and ensure availability for access via the web enabled architecture;
- develop a system to track and assess new and proposed initiatives associated with the maritime domain (it is incumbent upon each agency to inform the respective Hub of new programs and initiatives);
- maintain a directory of world-wide MDA-related capabilities, procedures, and ongoing activities for their respective MDA pillar;
- establish a process or protocol for communicating MDA-related needs, developments, and information to federal, state, local, tribal, private sector, and international stakeholders;
- coordinate interagency development of capability goals;
- identify issues that inhibit achieving MDA;
- advocate near-term improvements to information sharing that enhance fusion and analysis of maritime data by stakeholder agencies as the enterprise moves toward a SOA;
- maintain consistent liaison with other Enterprise Hubs, establish a formal quarterly summit to exchange needs, ideas, developments and standards;
- facilitate progress toward a net-centric architecture within their respective MDA pillar; and
- address the following areas and provide recommendations to the governing organization for common standards of
    - collection,
    - fusion/analysis,
    - dissemination,
    - archive/maintenance,
    - metrics,
    - data integrity, and
    - data security.

Due to the unique characteristics and subject matter expertise required of the net-centric MDA architecture, a lead federal agency to address architecture development, management, and maintenance was required. This agency functions in a similar manner to the Enterprise Hubs and is charged with the management and migration of these Hubs to a virtual environment. The lead federal agency serves as the MDA Director's subject matter expert for all network management and maintenance considerations and addresses the following requirements:

- Define architecture compatibility standards;
- Host or identify those who will host, net-centric enterprise services;
- Recommend associated technology investments;
- Enable the Service Oriented Architecture functionality;
- Manage network security and appropriate information assurance measures; and
- Maintain registries and provide identification, discovery, and access services.

There are currently four MDA Enterprise Information Hubs. The Cargo and People Information Hubs are led by U.S. Customs and Border Protection (within DHS). The Infrastructure Information Hub is led by the U.S. Office of Infrastructure Protection (within DHS). The Vessel Information Hub is led jointly by the National Maritime Intelligence Center, the Office of Naval Intelligence, and the Coast Guard Intelligence Coordination Center. The Maritime Domain Awareness Architecture Management Hub is led by the U.S. Navy.

(To read the entire U.S. National Concept of Operations for Maritime Domain Awareness please visit www.gmsa.gov)

Appendix C
GMISS 2009 Agenda

Version: Final 091409 1500

GLOBAL MARITIME INFORMATION SHARING SYMPOSIUM

September 15-17, 2009

National Defense University, Ft. McNair, Washington DC.

Streamlining Maritime Information Sharing

Improving Maritime Efficiency, Security, Safety and the Environment

MONDAY, 14TH SEPTEMBER (Check-in / Travel Day)

All Day	Arrival/Hotel Registration at Marriott Washington – Dupont Circle (1221 22nd Street NW)
1800-2100	GMISS Check In - No-Host Reception at Marriott Washington (Light Hors d'oeuvres & Cash Bar) On 2nd Level above Hotel Lobby.

TUESDAY, 15th SEPTEMBER (Conference Day 1)

0700-0715	Assemble in the Lobby of Hotel • *Assemble in hotel lobby for transport to Lincoln Hall, NDU. Ft McNair, Washington DC* • *Attire: business attire for all attendees (Civilian business attire preferred for uniformed personnel)*	
0715-0745	Transit from Marriott Washington Hotel to Lincoln Hall, National Defense University	
0700-0800	Continental Breakfast & Final Registration – NDU, Lincoln Hall, Rooms 1104, 1105,1107,1119	
0800-1145	**Plenary Sessions – "Industry & Government Perspectives on The State of Global Maritime Awareness"** *Full audience*	
0800-0810	"Conference Background, Rules & Goals"	Capt George McCarthy, USN, OGMSA Symposium Moderator
0810-0815	Keynote Introduction	Mr. Gary Seffel, Director, OGMSA
0815-0845	Welcoming Remarks – US Coast Guard	Vice Admiral David Pekoske, USCG Vice Commandant, US Coast Guard
0845-0850	Welcoming Remarks – NMIC	RADM Ann Gilbride, USN Director, National Maritime Intelligence
0850-0920	Introduction to the National Maritime Intelligence Center	RDML Roy Nash, USCG Deputy Director, National Maritime Intelligence Center

Streamlining Information Sharing

Improving Efficiency, Security, Safety and the Environment

0920-0930	Department of Justice Welcome	Ms. Sandra Webb Deputy Director Community Oriented Policing Services Department of Justice
0930-1000	International Trade Perspective	Mr. Steve Carmel, Senior Vice President, Maritime Services Maersk Line Limited
1000-1030	**Break/Refreshments – Lincoln Hall, Rooms 1105, 1107, 1119.**	
1030-1100	DHS Infrastructure Protection Perspective	Mr. Tom Watson, Director Infrastructure Coordination and Analysis Office of Infrastructure Protection Department of Homeland Security
1100-1130	Ship/Port Agents' Perspective	Mr. Jeffrey J. Milstein Director of Field Operations, Moran Office of Maritime & Port Security
1130-1145	Audience Comment Period	Symposium Moderator
1145-1245	**Lunch - NDU Lincoln Hall, Rooms 1105, 1107, 1119**	
1245-1500	**1st Panel Discussion - Lincoln Hall, NDU** *Topic: Establishing Efficient Means for Threat Warning Information Exchange between International Maritime Industry & Government.*	
1245-1300	Panel Welcome	Panel Moderator – Mr. Owen Doherty Director, Office of Security US Maritime Administration
1300-1315	Maritime Security Council Perspective	Mr. William Watson Board of Governors Maritime Security Council
1315-1330	Benchmarking Partners Perspective	Mr. Ted Rybeck Chief Executive Officer Benchmarking Partners
1330-1345	Industry Perspective	Mr. Eric Ebeling Director of Government Relations American Shipping and Logistics Group
1345-1400	OSAC Perspective	Mr. Mike Limpantsis, Acting Director, Overseas Security Advisory Council (OSAC) Department of State
1400-1500	Questions and Answers	Panel Moderator
1500 – 1530	**Break/Refreshments – Lincoln Hall Rooms 1105, 1107, 1119**	
1530-1730	**2nd Panel Discussion – Lincoln Hall, NDU** *Topic: Industry and Government issues and concerns with Maritime Information Sharing*	
1530-1545	Panel Welcome	Panel Moderator- Mr. Gordan Van Hook Senior Director, Maersk Line, Limited Innovation and Concept Development

1545-1600	Port/Maritime Security/Law Enforcement Perspective	Chief Michael Berkow Savannah-Chatham Metro Police
1600-1615	Office of the Director of National Intelligence	Mr. Alexander W. Joel Civil Liberties Protection Officer, ODNI
1615-1630	SEAHAWK Center Perspective	Mr. Frank Gutierrez, Former Deputy Director Project SEAHAWK
1630-1645	UK Perspective	Mr. Gavin Simmonds Shipping Defence Advisory Committee The Chamber of Shipping
1645-1730	Questions and Answers	Panel Moderator
1700-1715	***Spouses attending Officer's Club Social assemble in lobby of Washington Marriott for transportation to Fort McNair Officer's Club***	
1730	**End of Day 1 Working Sessions**	
1730	Walk to Ft. McNair Officer's Club – No Host Social	
1730-2030	Ft. McNair Officer's Club – No Host Social (Heavy Hors D'oeuvres)	
1745-2030	Shuttles/Bus transit from Ft. McNair Officer's Club front door to Washington Marriott	

No Further Organized Events this Day.

WEDNESDAY, 16th SEPTEMBER (Conference Day 2)

0700-0715	Assemble in Lobby of Washington Marriott Hotel • *Assemble in Hotel Lobby for transport to Eisenhower Hall, NDU. Ft McNair, Washington DC* • *Attire: business attire for all attendees (Civilian business attire preferred for uniformed personnel)*	
0715-0745	Transit from Hotel to Eisenhower Hall, NDU	
0700-0800	**Continental Breakfast – Eisenhower Hall, First Floor, Room 107**	
0800-1145	**Plenary Sessions – "Industry/Government Dialog – Digging Deeper"** *Full audience – Eisenhower Hall, Baruch Auditorium*	
0800-0805	Administrative Remarks	Symposium Moderator
0805-0830	"MDA for America and Beyond"	RDML Dennis FitzPatrick N3 Joint Operations Director U.S. Fleet Forces Command
0830-0900	International Maritime Industry Perspective	Mr. Phillip J. Shapiro President & Chief Executive Officer Liberty Maritime Corp
0900-0920	U.S. State Department Counter-Piracy Perspective	Mr. Andrew Shapiro Assistant Secretary of State for Political-Military Affairs U.S. Department of State
0920-0950	Voyage Risk Assessment	Mr. Giles Noakes, Head of Security Dept.

0950-1000	Audience Comment Period	Baltic & International Maritime Council Symposium Moderator
1000-1030	**Break/Refreshments, Eisenhower Hall, First Floor, Room 107**	
1030-1100	Customs & Border Protection Perspective	Mr. Frank Jaramillo, Director National Targeting Center (Cargo) Customs & Border Protection Department of Homeland Security
1100-1130	LNG Shipping Perspective	Captain Mark Lane, Senior VP Operations Excelerate Energy, LLC
1130-1145	Audience Comment Period	Symposium Moderator
1145	Walk to Ft. McNair Officer's Club – Keynote Luncheon	
1200-1300	**Luncheon – Keynote Speaker – Ft. McNair Officer's Club, Crystal Ballroom, 2nd Deck** Mr. David T. Matsuda Deputy Maritime Administrator, U.S. Department of Transportation	
1300-1500	**Break Out Session #1** *Three topics below will be presented twice – attendees should participate in two topics relevant to the Working Group they are planning to attend on Day 3.*	

Topic #1 **Changing Frameworks: Interconnecting Maritime Centers into a Global Grid.**

- *"Getting the right information to those who need it, quickly."*

ROOM ASSIGNMENT: Lincoln Hall, Room 1105, NDU

Session Moderator – Captain Russell Pegg, UK Royal Navy (confirmed)

1300-1310	Introductions	Session Moderator
1310-1325	Maritime Exchange Perspective	Mr. John E. Veentjer Executive Director Marine Exchange of Puget Sound
1325-1340	Singapore MDA Perspective	COL Chua Meng Seng, Deputy Commander MSTF Republic of Singapore Navy
1340-1355	MAOC Perspective	Mr. Conor Shields, Manager Maritime Analysis and Operations Center Lisbon
1355-1410	NMSAC Perspective	Captain Mike Rodriguez International Association of Masters, Mates and Pilots
1410-1500	Questions and Answers	Session Moderator

Topic #2 **Changing Perceptions: Increasing Industry & Government Dialog Points.**

- *"Increasing the level of understanding of each other's MS/MA issues and concerns."* Using the increasing open sharing of AIS & merchant vessel locations as an example.

ROOM ASSIGNMENT: Lincoln Hall, Room 1107, NDU

Session Moderator – Mr. Lennis Fludd, Maritime Administration (confirmed)

1300-1310	Introductions	Session Moderator
1310-1325	Marine Offshore Industry Perspective	Mr. Ken Wells, President Offshore Marine Service Association
1325-1340	Ocean Policy Development & Marine Spatial Planning	Dr. John Oliver Senior Ocean Policy and Programs Advisor Office of Policy Integration (CG-53) U.S. Coast Guard
1340-1355	USCG AIS Data Sharing Policy	CAPT Curtis L. Dubay (Ret.), P.E. Office of Maritime Domain Awareness and Information Sharing (CG-51-M)
1355-1410	Maritime Information Sharing Task Force	Ms. Wendy Walsh, Naval Postgraduate School
1410-1500	Questions and Answers	Session Moderator

Topic #3 **Changing Policies: Increasing Industry Involvement in Policy Making.**

- *"Partnering Industry and Government to mutually beneficial Policies.* Using International Governments piracy policy development as an example.

ROOM ASSIGNMENT: Lincoln Hall, Main Auditorium, NDU

Session Moderator – Mr. Joseph J. Cox, President & CEO, Chamber of Shipping of America

1300-1310	Introductions	Session Moderator
1310-1330	Maritime Industry Perspective	Mr. James Christodoulou Chief Executive Officer Industrial Shipping Enterprise
1330-1350	USCG Perspective	Mr. Dana Goward, Office of Maritime Domain Awareness and Information Sharing (CG-51-M) U.S. Coast Guard
1350-1410	"Armed Security Pitfalls"	Mr. Charles Papavizas, Esq. Partner Winston & Strawn, LLP
1410-1500	Questions and Answers	Session Moderator
1500-1530	**Break/Refreshments – Lincoln Hall Rooms 1105, 1107, 1119**	

1530-1700 **Break Out Session #2**
The aforementioned three topics will be repeated, attendees should participate in a second topic.

Topic #1 **Changing Frameworks: Interconnecting Maritime Centers into a Global Grid.**

- *"Getting the right information to those who need it, quickly."*

Session Moderator – Captain Russell Pegg, UK Royal Navy

Topic #2 **Changing Perceptions: Increasing Industry & Government Dialog Points.**

- *"Increasing the level of understanding of each other's MS/MA issues and concerns."*

Session Moderator – Mr. Lennis Fludd, Maritime Administration

Topic #3 **Changing Policies: Increasing industry involvement in Policy Making.**

- *"Partnering Industry and Government to mutually beneficial Polices."*

Session Moderator – Mr. Joe Cox, President & CEO, Chamber of Shipping of America

1700	**End of Day 2 Working Sessions**
1700-1745	Bus Transit from Lincoln Hall, NDU to Washington Marriott – Dupont Circle
1900-2200	Gala Dinner – Washington Marriott – Dupont Circle (Sit-Down Dinner & Cash Bar)

THURSDAY, 17th SEPTEMBER (Conference Day 3)

0700-0715	Assemble in Lobby of Washington Marriott Hotel • *Assemble in Hotel Lobby for transport to Lincoln Hall, NDU. Ft McNair, Washington DC* • *Attire: business attire for all attendees (Civilian business attire preferred for uniformed personnel)*	
0715-0745	Transit from Hotel to Lincoln Hall, National Defense University	
0700-0800	**Continental Breakfast – Lincoln Hall, NDU Rooms 1105, 1107, 1119**	
0800-0815	Plan of the Day/Administrative Notes	Symposium Host
0815-0830	Attendees proceed to individual working group rooms.	
0830-1230	**Working Groups Sessions / Working Lunch** *Working group sign-up during registration or at Command Center.*	
1130-1230	*Lunch is available for working groups – Lincoln Hall Rooms 1105, 1107, 1119*	

Working Group A: Building a Global Maritime Information Exchange Grid - Is It Possible ?

Room Assignment: ***Lincoln Hall, Room 1105, NDU***

Recommended Attendees: Technical, Operational, Systems, Ports, Law Enforcement.

Discussion Topics: Bringing together Maritime Operation Centers, Fusion Centers, Maritime Exchanges, Government Maritime Information Hubs into a single grid. Creating a universal Dial String for Mariner Access to Regional Maritime Centers, US Government Interagency System Collaboration Efforts.

Lead: Captain Andy Bjork, USN, USFF *Co-lead: Capt Ralph Nieves, USN, OGMSA Data Sharing & Infrastructure*

0830-0840	Working Group Introductions/Organization	Lead/Co-Lead
0840-0850	New Zealand Perspective	Mr. Richard Davies, Manager National Maritime Coordination Centre New Zealand Customs Service
0850-0900	Canadian Perspective	Mr. Tom Fredericks Marine Security Operations Centre (East)
0900-0910	Single Web Portal Access to	Mr. Robert Hall, Jr.

	US Government Information	Maritime Architecture Lead National Maritime Intelligence Center Office of the Director of National Intelligence (ODNI)
0910-1230	Working Group Discussions	Lead/Co-Lead

Working Group B: Bridging the Understanding Gap Between Maritime Industry & Government
Room Assignment: ***Lincoln Hall, Room 1107, NDU***

Recommended Attendees: Maritime Associations, Government Policy personnel Maritime Education, Training, Manning, Marketing, Maritime Government Liaisons.

Discussion Topics: How can we facilitating deeper industry access to maritime policy formulation process ? What industry input is presently obtained in the process ? Who singularly represents the international maritime industry to the US Government ? Are maritime training for Intelligence analysts, internships, maritime awareness courses a way ?

Lead: Mr. Andy Grasso, American Roll-on, Roll Off Carriers *Co-Lead: CDR James Feldkamp, USN, OGMSA*

0830-0840	Working Group Introductions/Organization	Lead/Co-Lead
0840-0850	Inter-Agency Investment Strategy Report	Captain Dale Ferrier, USCG, OGMSA Branch Chief – Policy Branch Office of Global Maritime Situational Awareness
0850–0900	USCG Centers of Expertise	Captain Gordon Loebl, USCG Chief, Office of Quality Assurance & Traveling Inspectors (CG-546) U.S. Coast Guard
0900-0910	Maritime Training Perspective	Mr. John Tomoney Global Maritime & Transportation School U.S. Merchant Marine Academy Kings Point, NY
0910-1230	Working Group Discussions	Lead/Co-Lead

Working Group C: Resolving Information Privacy, Proprietary & Classification Concerns.
Room Assignment: ***Lincoln Hall, Room 1119, NDU***

Recommended Attendees: Maritime Attorneys, Government Policy personnel, Intelligence community.

Discussion Topics: Government clearances for maritime personnel, lack of trust and reciprocity with information sharing between governments and industry, information sharing dispute resolution.

Lead: Mr. Tim Phillips, GMAII *Co-Lead: Name: Capt David Sanders, USN, OGMSA Policy Branch*

0830-0840	Working Group Introductions/Organization	Lead/Co-Lead
0840-0850	"USG Barrier Resolution Process"	Captain David Sanders, USN, OGMSA
0850-0900	Maritime Industry Perspective	Mr. Paul Londynsky Matson Navigation Company, Inc.
0900-0910	"AIS Coverage, an Industry/government Co-op ?"	Moses Calouro, President Maritime Information Systems, Inc.

0910-1230	Working Group Discussions	Lead/Co-Lead

Working Group D: Piracy: A Model of Co-developed, Mutually Beneficial Policies?
Room Assignment: ***Lincoln Hall, Auditorium***

Recommended Attendees: Vessel Operators, Risk Management, Navy & Coast Guard Personnel.

Discussion Topics: How well has the world responded to Piracy ? Do the policies fit the issue ? Can the Piracy response model be utilized to respond to other maritime crisis ? What if piracy occurs elsewhere, do we have to re-invent the response ?

Lead: Mr. Giles Noakes, Head of security Dept, BIMCO *Co-Lead: LCDR Eric Huemme, USN, OGMSA*

0830-0840	Working Group Introductions/Organization	Lead/Co-Lead
0840-0850	BIMCO Perspective	Mr. Giles Noakes Head of Security, BIMCO
0850-0900	USCG Security Directive & IMO Guidelines	Mr. Charles (Bud) Darr, USCG Office of Maritime & International Law
0900-0910	U.S. Maritime Administration Perspective	Mr. Owen Doherty Director, Office of Security US Maritime Administration
0910-1230	Working Group Discussions	Lead/Co-Lead

1300-1500 **Feedback Sessions – Working Group Consensus**
"Identifying the Road Ahead"

Goal – Each Working Group to present a two-slide summary of their 'points of discovery.' Each Working Group to identify three (3) specific, measurable action items to be engaged in the next 6 months [Oct 09 – Mar 2010].

1300-1310	Ground Rules	Symposium Moderator
1310-1330	Working Group Recommendations	WG A Lead as Selected
1330-1350	Working Group Recommendations	WG B Lead as Selected
1350-1410	Working Group Recommendations	WG C Lead as Selected
1410-1430	Working Group Recommendations	WG D Lead as Selected
1430-1500	Full Audience Voting on MA/MS Priorities	
1500-1530	Closing Remarks	Mr. Gary Seffel, Director OGMSA
1530	Transit from Lincoln Hall to Local Airports, Union Station or Washington Marriott Hotel	

== End of Conference ==

Appendix D
Summary of GMISS 2009 Presentations

The following are the summarized excerpts of individual presentations and follow-on discussions as transcribed at GMISS 2009 by OGMSA team members. They are not intended to represent all that was stated, presented or discussed, nor to indicate that inclusion or exclusion of a specific concept or statement represents the speaker's position or priorities. Summarized excerpts as transcribed by OGMSA are combined with participant comments as entered by the participants into the collaborative software during GMISS 2009. These comments may not accurately reflect what was being stated, presented or discussed.

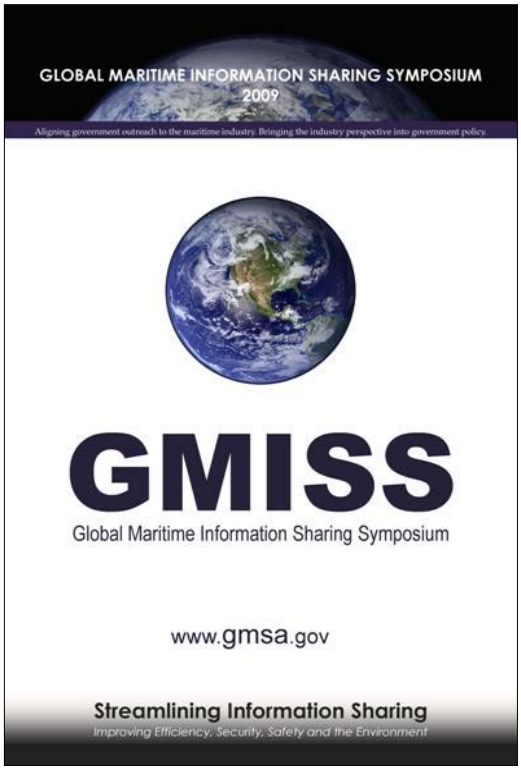
These summary excerpts and comments are being provided for general discussion and should in no way reflect on the speakers or any individual participant.

Plenary Sessions and Keynote Speakers

Welcoming Remarks

Opening Remarks

Captain George E McCarthy, USN
Chief, Outreach and Coordination Branch
Office of Global Maritime Situational Awareness (OGMSA)
www.gmsa.gov



Good Morning, welcome and thank you for honoring us with your time and participation in this, the second year of the Global Maritime Information Sharing Symposium (GMISS). A special thank you to the National Defense University for this incredible venue and to our other hosting agencies which will each be welcoming you this morning, for helping us keep your attendance costs to a minimum.

The Office of Global Maritime Situational Awareness (OGMSA), this event's organizer, was itself stood-up as an office in August of 2007 for the purpose of increasing the open sharing of global maritime information to the improvement of national security. Two facts quickly became apparent. One: greater open maritime information exchange would also benefit maritime safety, commerce and the environment in addition to security. Two: little of this monumental undertaking would be achievable without the involvement of the international maritime industry.

To ensure the full involvement of industry and to help bridge the gap of understanding between industry and government, the GMISS five-year program of annual symposia was created to help government gain a better understanding of the subtleties of the international maritime world and to help industry gain a better understanding of the very legitimate concerns of those responsible for national or maritime security.

In your welcome materials are the summary results of a number of prior government maritime industry outreach conferences. Each reached similar conclusions:

- Damage to any portion of the Global Supply Chain can seriously affect whole economies. Imagine the result if several ports get damaged at once.
- The need for immediate recovery of the Global Supply Chain in the event of damage requires proactive policies in place, and understood, ahead of time.

- There should be a single point of contact within government for the maritime industry to report suspicious behavior to, while also being able to receive vital security information in return.
- Can we not coordinate the exchange of needed information?
- Can the government consolidate or coordinate these outreach conferences towards coordinating their message?

This year's GMISS Agenda is a reflection of those findings.

The government needs to involve industry more, and the industry needs to become more involved. Both require an increased level of dialog and trust. The purpose of this symposium is to create new relationships between the international maritime industry and those in the government involved in maritime security, awareness and the necessary information exchange in support thereof.

What we want out of this symposium is to bridge the understanding gap between the maritime industry and government to facilitate the development of mutually beneficial outcomes. It begins with educating each other about what works and what does not with regard to more secure oceans and more efficient trade. These cannot be mutually exclusive. Without industry involvement, while the policies may ensure greater security, they could be at the expense of efficient commerce. Conversely, commerce cannot prosper long without security.

This symposium's approach is unique. You will hear a diversity of opinions from the domestic and international maritime industry, navy, coast guard, law enforcement and intelligence personnel. Beginning with plenary presentations, we finish up with short presentations developed in this symposium by working groups whose findings will continue to be worked on by representatives from both industry and government throughout the year.

When developing the agenda, I made it a point to try and match up alternative views of the matter being discussed, be it threat warning, linking maritime centers, privacy, the use of AIS[9] etc. If this results in your making new professional connections, then we have succeeded. If it results in your finding a new enemy, well then feel free to make use of our very own conference resolution tools (*Note: CAPT McCarthy held up boxing gloves*).

While piracy is discussed as part of this symposium, it is as a symptom of the need for a greater understanding between those that trade across oceans and those that wrestle with the policies to ensure their safety and security. Today's hot issue may or may not be piracy, depending on your vantage point, but it is this symposium's purpose to establish dialog and standards in preparation for tomorrow's possibilities, be they positive or negative in effect. Either way, let us at least agree from this point forward that if we are to continue to share the world's waterways, then we must share the task of making them safer, more secure, and commercially effective through mutually beneficial policies and solutions. These are clearly shared responsibilities regardless of your vantage point.

The ground rules for this symposium are equally simple: speak up, argue, be heard, but please no retribution. Mutual benefit is the desire. Therefore trust must be present.

---

9 Automatic Identification System. AIS is a maritime navigation safety communications system standardized by the International Telecommunication Union (ITU) and adopted by the International Maritime Organization (IMO) that provides vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft; receives automatically such information from similarly fitted ships; monitors and tracks ships; and exchanges data with shore-based facilities. Source: Electronic Code of Federal Regulations, http://ecfr.gpoaccess.gov.

A brief note on the hidden value in subtleties: the closest translation in French for “Awareness” is the statement “une conscience plus profonde (pour tout),” which in English means, “a deeper consciousness for all.” I challenge both the maritime industry government to take advantage of this time at GMISS to achieve a new level of consciousness of each other’s issues and concerns. This is the path to greater maritime awareness.

And now, please join me in welcoming the Director of our Office of Global Maritime Situational Awareness, and my boss, Mr. Gary Seffel.

OGMSA Welcoming Remarks

Mr. Gary Seffel
Acting Director
Office of Global Maritime Situational Awareness (OGMSA)
www.gmsa.gov

This is our second GMISS. We have implemented many of the recommendations for improvement made during last year's GMISS. Once again, we request your feedback for improvement to make this symposium the most effective it can be.

Thanks to those making presentations at our symposium; your input is essential to informing our discussions with a common understanding of the varied perspectives inherent in this complex system. When we first started carrying mobile phones, we never imagined all the applications they would place in our hands. Maritime Domain Awareness (MDA) is generally associated with maritime security. We have already found unexpected benefits of maritime information sharing.

When the US Airways flight landed in the Hudson River early this year, an engine sheared off. Finding it was essential to the investigation, which of course leads to improved safety. The bottom of the Hudson River in that area is covered in metal – old cars, washing machines, etc. But a sonar scan of the bottom had been recently conducted for environmental uses. The people who collect environmental information shared the results with the people who collect safety information. All they had to do is run another scan and look for the anomaly, and they quickly recovered the engine.

We don't know where maritime information sharing will take us – and clearly we have to be careful that it is not misused. But we can't even imagine the benefits we will eventually reap from what we accomplish here in the next three days.

U.S. Coast Guard Welcoming Remarks

Vice Admiral David Pekoske
Vice Commandant
U.S. Coast Guard
U.S. Department of Homeland Security
www.uscg.mil

Welcome to the Global Maritime Information Sharing Symposium. There should be a single point of contact within government for the maritime industry to report suspicious behavior to, while also being able to receive vital security information in return. There is a need to streamline information sharing between the government and private sector in the Maritime industry. By sharing information, both sectors are able to gain greater situational awareness. Cooperation between the government and

private sector are needed to safeguard the maritime information system, continue balance of safety and security, and ensure our capabilities and capacities are keeping pace with changes in the transportation system. To meet these challenges and changes, the Coast Guard is going through a signification modernization. The USCG desires to be an organization that is constantly adjusting in response to environment and maritime needs.

Participant Discussion:

- **Seahawk is another silo**, like law enforcement drug task forces in 1980s. Need to interact with intermodal, not just security. As the Coast Guard stands up IOCs we are looking at a broader model, working with (DHS) Secretary Napolitano to expand the scope. If silos exist between interagency operations at ports, no agency is able to do its job effectively. It's important that the federal government work with the state and local agencies as well as the port operations to adequately protect the port. People get concerned about the risks of working outside the envelope. You have a bigger risk by not expanding your view.
- **Local police find themselves communicating with many different agencies** on the federal level, reporting to many of them the same information on one problem –this problem needs to be resolved so that local enforcement agencies are not spending so much time filing reports.
- **Who's in charge of MDA?** Why hasn't USCG taken the lead? The creation of OGMSA has provided the federal government with an office with leadership in the area of maritime domain awareness (MDA). With USCG's move from the Department of Transportation to the Department of Homeland Security, the urgency in regards to MDA was lost. Now the focus needs to be on sharing information between agencies and the private sector. The government stood up OGMSA and fusion centers to coordinate with other agencies. You can't say I'm in charge and then have a collaborative solution. We'll have a lead role, but you won't see anyone who says "I'm in charge."
- **Is piracy a crime or terrorism?** (Additional participant discussion followed regarding piracy/terrorism and the need to raise the overall competency of organizations like the USCG to handle threats to security.) There are border security and maritime security issues that are in play. The Coast Guard is developing the same skills used in counter drug –working with global partners to implement and expand those skills with this in mind. There is a need for international cooperation in raising Maritime Security to a higher level. Coast Guard is improving in that area, and still has a lot of progress to make. Can all acts of terrorism be prosecuted as crime – transnational organized crime? Judicial capacity-building is an important aspect of the conference agenda, because so much of the information used in cases will be originating in other countries – why can't that information be included in the information sharing for threat reduction? There is a need, and it's missing from the GMISS agenda, to engage with other countries to address this problem.
- **Often my TWIC[10] card is not recognized at airports.** It's all part of DHS – it should be recognized. TWIC is still improving with biometric recognition.
- **Centers of Excellence are a great concept** – a tool to develop a better regulator for industry. Get these folks to understand the industry; example: the "methane monster" is not the risk it is often portrayed as. As far as COE's[11], if you think senior officials that represent the Coast Guard in your port lack important information, invite them aboard. They will come learn, not only the specifics of your industry, but also the high level of professionalism of the mariners.

10 The Transportation Worker Identification Credential (TWIC) was established by Congress through the Maritime Transportation Security Act (MTSA) and is administered by the Transportation Security Administration (TSA) and U.S. Coast Guard. TWICs are tamper-resistant biometric credentials that will be issued to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities and all credentialed merchant mariners. Source: Transportation Security Administration, www.tsa.gov.

11 National Centers of Expertise (NCOE). Independent analysis recognized the need for a targeted revitalization of technical competency and expertise within marine safety to keep pace with ever-increasing growth and complexity in the maritime industry. NCOEs provide key venues for professional development and exchange between industry and Coast Guard personnel. By focusing on specialized areas of industry and enhancing Coast Guard capabilities, NCOEs improve inspector and investigator competencies while promoting nationwide consistency. Source: U.S. Coast Guard, ALCOAST 131/09, COMDTNOTE 16700.

National Maritime Intelligence Center Welcoming Remarks

Rear Admiral Ann Gilbride, United States Navy
Director
U.S. National Maritime Intelligence Center (NMIC)
www.nmic.navy.mil

On behalf of the National Maritime Intelligence Center, welcome to GMISS. There must be an awareness of each other's contributions in making efficient global trade a reality. Your participation in GMISS is appreciated.

Participant Discussion:

- There are numerous concerns about how to better coordinate information and intelligence sharing from the shipping industry and port authorities to government, concerns about intelligence sharing from federal resources like the NMIC to local law enforcement. Specifically, some of us are concerned that the Coast Guard's decision to transfer its MDA function to CG-2[12], where SIPRNET[13] is used and SCI[14] clearances are required. This will not bode well on sharing intelligence and information with local law enforcement and industry.

Department of Justice Office of Community Oriented Policing Services Welcoming Remarks

Ms. Sandra Webb
Deputy Director
Office of Community Oriented Policing Services (COPS)
U.S. Department of Justice
www.cops.usdoj.gov

COPS is happy to be involved again in GMISS. COPS uses information sharing and grant resources to improve community policing – looking at the tools needed to prevent crime and committing grant resources. COPS provided scholarships to law enforcement and fusion centers to bring input to the solutions you will develop at this event. COPS works with the Department of Homeland Security, PM-ISE[15], OGMSA, and International Chiefs of Police to better coordinate information sharing. For example, we're working on eliminating classification barriers with state and local law enforcement. There are

12 Coast Guard Intelligence and Criminal Investigations.

13 Secret Internet Protocol Router Network – a federal government network for information classified at the Secret level. Information shared on the SIPRNET cannot be subsequently shared on unclassified networks until cleared.

14 Sensitive Compartmented Information (SCI) refers to the handling methods of certain types of classified information, and the designation of individuals authorized to access such information.

15 The Program Manager for the Information Sharing Environment. In response to the 9/11 Commission's Recommendations, the Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act of 2004. Section 1016 of the law called for the creation of an Information Sharing Environment and defined it as "an approach that facilitates the sharing of terrorism information." The law required the President to designate a Program Manager for the ISE. and establish an Information Sharing Council to advise the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among Federal departments and agencies participating in the ISE. Under the Obama Administration, the Information Sharing Council has been integrated into the White House policy process through the Information Sharing and Access Interagency Policy Committee (IPC), so that the work of the ISC will move forward under the auspices of the Executive Office of the President. Source: ISE, www.ise.gov.

resources available at the COPS Website[16]. COPS also promotes cooperation between law enforcement and private security – 85% of infrastructure protection is provided by private security.

Keynote Speakers

Gala Dinner Keynote Speaker

Mr. John Porcari
Deputy Secretary
U.S. Department of Transportation
www.dot.gov

On behalf of Secretary LaHood[17], thanks for coming and for your participation. The maritime system is a critical piece of our transportation network. If it goes perfectly, nobody notices. If not, they want to know why.

We recently marked the 8th anniversary of 9-11 and a key lesson was that sharing information is one of the most important steps we can take. We've made significant steps in that area at the Maritime Administration. One example is the piracy section of the MARAD Website[18]. With MarView[19], the Department of Transportation has emerged as a leader of information sharing for your industry. We need your input.

Before coming to the Department of Transportation, I did two tours with the Maryland Department of Transportation. For the Port of Baltimore, I was in that role on 9-11. Unlike other states, Maryland puts everything under one roof as far as transportation. One of the best things going for us was our working relationship with the Coast Guard and our private sector partners. What really matters is how we work together to build bridges. Baltimore was the first major port to institute TWIC – and we lived through it. I wouldn't volunteer for that a second time. TWIC is a great example of a security measure that's not fully implemented.

Gatherings like GMISS are critical to define where we go together. I look forward to working with all of you. DOT is your partner. My door is always open. Your input is critical to our nation's security. I look forward to working together.

16 http://www.cops.usdoj.gov/

17 The Honorable Ray Lahood, Secretary, U.S. Department of Transportation.

18 www.marad.dot.gov.

19 Marine View. www.marview.gov. MarView is an integrated, data-driven environment providing essential information to support the strategic requirement of the U.S. Marine Transportation System (MTS) and its contribution to the economic viability of the nation. MarView provides the ability to fuse data together to create models and simulations for capacity planning, economic impact analysis, on-demand forecasting, and plans for mitigating and reacting to emergency situations. Capabilities include Crisis Tracking and Emergency Notification (CTEN), geospatial information on the MTS and intermodal transportation, a distance calculator, innovative electronic collaboration rooms, and business intelligence tools for data analysis and data manipulation. Access to MarView is granted through a free subscription. Source: Maritime Administration, www.marview.gov.

Luncheon Keynote Speaker

Mr. David Matsuda
Deputy Maritime Administrator
U.S. Maritime Administration (MARAD)
U.S. Department of Transportation
www.marad.dot.gov

I would like to thank the Secretary of Transportation[20] and OGMSA for inviting me to speak at this luncheon. The mission of MARAD is to be a strong advocate of the maritime industry. We are uniquely positioned to work with stakeholders – private, state, local and federal. MARAD holds a fleet of additional ships for times of emergencies and is the administrator of the U.S. Merchant Marines. MARAD is also assisting in port expansion, currently working on the port in Anchorage, Alaska.

The MARAD MarView program is a Web-based portal, assisting in decision-making processes. It can be used to find details on ships, allowing for quick and accurate data in real time. It is also used to find lost vessels, such as during Hurricane Ike. Please take a virtual tour at www.marview.gov.

MARAD is aiding in preventing international piracy, and information is key to this challenge. MARAD is working with the U.S. Coast Guard, the U.S. Navy and nations worldwide to address this problem. The National Maritime Intelligence Center will be able to monitor MARAD reports on piracy and other maritime issues.

Industry and Government Perspectives on the State of Global Maritime Awareness

Introduction to the National Maritime Intelligence Center

Rear Admiral Roy Nash, United States Coast Guard
Deputy Director
U.S. National Maritime Intelligence Center (NIMC)
www.nmic.navy.mil

National Maritime Intelligence Center[21] (NMIC) is eight months old, established by an interagency intelligence working group. Why is there a need for a National Maritime Intelligence Center? The maritime environment is growing in importance. It includes a dynamic land-sea interface with ocean-going ships, the shipping industry, passengers and crew, and small vessels. The oceans are the largest ungoverned space on the planet and with all this ungoverned space, narco-traffickers, oil smugglers, and pirates are able to exist. Highly adaptive adversaries are innovative, flexible and agile. They include pirates, terrorists, and criminals.

20 The Honorable Ray Lahood, Secretary, U.S. Department of Transportation.

21 NMIC is one of three co-leads for the Maritime Domain Awareness Vessel Information Hub, along with the Office of Naval Intelligence and the Coast Guard Intelligence Coordination Center. The U.S. National Concept of Operations for Maritime Domain Awareness recommended creating hubs to coordinate the flow of specific types of information while a global maritime information sharing network develops. For more information on MDA Enterprise Hubs, please see Appendix B.

The National Maritime Intelligence Center functional areas derived from strategic guidance include:

- Plans and Program Requirements Integration
- Technology Innovation
- Architecture
- Analysis Integration
- Collection Integration
- Information Management and Sharing

NMIC Roles and Responsibilities include:

- Developing integrated strategies
- Working with interagency, international, industry, and private sector partners
- Investing in transformational research
- Advocating for maritime domain issues

The mission of the NMIC is to dynamically integrate the global maritime community for decision advantage by delivering unprecedented access for intelligence and information sharing, harnessing technology through innovation, speeding solutions and advocating for synchronized maritime requirements and investments. The way ahead for NMIC and maritime awareness issues is to continue interagency outreach.

Participant Discussion:

- There is a greater need for coordination of intelligence agencies. Is NMIC in charge of MDA? There is no one agency in charge of information sharing. It is a collaborative effort.
- How do companies provide feedback into the intelligence network? Companies want to be partners in intelligence. That is something we are at GMISS to work through. We are having this conference as a venue to become a better advisor on these issues.

International Trade Perspective

Mr. Steve Carmel
Senior Vice President, Maritime Services
Maersk Line, Limited
www.maersklinelimited.com

Maritime security must respect the interconnectedness of global commerce. Global trade is a source of global interconnectedness and a source of global conflict. It is instructive to remember that the causes of World War One and its continuation in World War Two are rooted in discontinuous evolutions in transport and information technology and the reaction of the landed class in Germany to the resulting competition. Interactions of people across borders in complex processes such as trade where there are always winners and losers can lead to unexpected outcomes, sometimes including instability and

conflict. A failure to properly prepare for a rapid recovery is likely to be as disruptive as a prolonged downturn. My remarks are thus oriented towards the more normal state of affairs that prevailed before the current downturn and to which we will return.

Despite the global recession and the increase of fuel prices, globalization is alive and well. While recovery from the current economic situation will happen quickly, uneven recovery across the globe will cause an upheaval in the global balance of power. The world is complex and now operates in networks of networks no one really understands. Much of the current turmoil is related to linkages propagating risk no one really appreciated until it was too late. Turmoil creates opportunity. The military pays much attention to asymmetric threats, but seems to afford less analysis to asymmetric opportunities. Others will exploit those we don't.

The Russians rely on pipelines to export their oil, though real influence on global oil prices requires tanker transport. Therefore, Russia began a pipeline from the Siberian oil fields to the Pacific Ocean. The global economic downturn left Russia unable to complete it. China recognized the opportunity and offered to fund continued oil field development and the pipeline, but it will now bring the oil to a Chinese refinery complex. Siberian oil fields cannot be taken off line at will. Russia becomes locked into providing an uninterrupted supply of oil to China, free from interdiction. This helps Chinese deal with what they call their "Malacca problem" or the ability of the U.S. to interdict the flow of oil destined for China via the sea. When you stitch together enough asymmetric opportunities, you get strategic surprise.

Current globalization is driven by disaggregation of the supply chain and exploitation of economies of scale and comparative advantage at ever-smaller levels of the production process across a wider swath of the globe. It is like an endless system of conveyor belts; goods are always in motion from where they enter the system to their final destination. If there is any break anywhere then the whole system stops. There is no distinction between domestic or international supply chains, nor mode of transport. Instability in remote parts of the world gets transmitted to main street USA much more frequently and with much greater speed than ever before.

U.S. military operations are very much dependent on the global supply chain functioning properly. Not just for delivery of finished goods, but more importantly to get them made to begin with. It is the nature of trade in component level material that the "made in" label is becoming increasingly meaningless.

We talk about the global supply chain as some monolithic thing and policy tends to treat it that way. That is not the case. The combination of containerized transport and the information systems needed to manage the global trading system have led to the disaggregated system of production that exists today where much trade is in component level intermediate goods rather than finished goods ready for retail. The proper functioning of many aspects of the global supply chain is highly dependent on information, making the global supply chain vulnerable to attacks on information infrastructure.

During the recent financial meltdown, trade was disrupted due to the lock up in the letter of credit market. A large-scale failure in the global information infrastructure will potentially have the same effect.

Trade in services, about 19% of global trade, is universally dependent on the global information infrastructure. Services could surpass merchandise as a percentage of total trade in the next decade. Services are a dominant U.S. export, in which it is a world leader, so the security of the global supply chain in services should not be overlooked. It is "transported" across a fiber optic backbone that is far

more vulnerable to disruption than most realize. Therefore, imagine our vulnerability to the impact of one marginally sober skipper on a scallop boat[22].

The U.S. is at least 80-percent dependent on imports for 21 critical strategic minerals. Kazakhstan supplies 50 percent of U.S. titanium. The U.S. is completely dependent on imports for 17 critical strategic minerals. China is the largest supplier to the U.S. of six of those 17. China passed Germany last year as the world's largest exporter - the U.S. is third - and has surpassed Canada as the largest source of U.S. imports. China is also the single largest destination for U.S. containerized exports moving by water. The U.S. remains the world's third largest exporter, and in terms of overall manufacturing, remains the world's largest manufacturer. China is more aptly described as an assembler vice manufacturer. The U.S. remains one of the world's largest exporters with nearly 10 percent of global exports. Because of this, and the fact that more than half of what the U.S. imports in containerized trade is component-level stuff destined for U.S. factories, disruptions to the global supply chain, or the U.S. component of it, either from bad guys or self-inflicted wounds will quickly be felt in the heartland in lost jobs.

The global supply chain is a very large complex system where little is black and white. Policy focus tends to be on very narrow parts of it. I'm not sure the complexity of the global supply chain is understood at the policy level, which in and of itself is a threat to the global supply chain. Policy is being made that effects the functioning of the system without appreciation for what those effects will actually be.

A great example was the Dubai Ports World debacle, blocked on the grounds of national security. The U.S. military depends the cooperation of Dubai Ports World, which controls ports such as Jebel Ali where much of the cargo bound for Iraq is transshipped to feeder ships in the commercial transport system. If they wanted to hurt us they could do it far more effectively over there. Another example was blocking the China National Offshore Oil Corporation from acquiring Unocal on national security grounds, which prompted instead the Chinese acquisition of a Kazak oil company headquartered in Canada which also had some Canadian tar sand holdings. This also moved China forward in dealing with its Malacca problem and expanded Chinese oil holdings in North America.

A major focus of GMISS is threats to the maritime trading system. The instant reaction is to focus on the bad guys. There are other threats such as congestion. Lack of capacity to handle peak volumes or allow for flows to be rerouted is a serious concern that never seems to make it into the debate. Congestion is the bad guys' force multiplier. It vastly amplifies anything he does, increases the likelihood that he will be successful, ensures that even if he is not successful there will be a fear reaction in related markets such as financial markets which is his primary goal, and ensures effects will be felt far beyond the immediate target area, drawing much desired publicity in the process.

There is little distinction between the global and domestic supply chains in trade in fungible commodities such as oil. Prices globally equilibrate quickly so a disruption affects prices everywhere. Rail capacity in the U.S. is operating near its limits. If you asked a reasonably well informed Chinese businessman what concerns him the most I would not be surprised if he did not say it was the U.S. Navy in Guam, but the state of our railroad system, which has a large impact on the Chinese economy since it is how Chinese imports move off the coast to their final destination.

The U.S. under invests in transportation infrastructure on the order of $20 billion a year according to the Congressional Budget Office. In order to just maintain the level of transportation capability we have now in the U.S. we would need to invest $20 billion a year more than we currently do. An alternative way to

22 Commercial scallop fishing is generally conducted by towing a large steel frame called a "drag" through scallop beds on the sea floor to rake the scallops into an attached "bag." Many of the communications between continents are conducted via fiber optic cable strung along the sea floor.

look at it is that every year, $20 billion in damage is done to our transportation infrastructure that nothing is done about. It is ironic that we spend so much money defending against threats to the supply chain that have never actually happened while allowing that supply chain to be attacked every day in a less spectacular but far more damaging way with no action. That amplifies the congestion problem, meaning we make the bad guys more potentially effective every day.

The structure of the global containerized transport system introduces vulnerabilities. Goods are inventory in transit, scheduled into production runs long before they arrive. There is little tolerance for disruption. The global system is a complex adaptive system structured as a scale-free network[23]. Scale-free networks are robust to random failures but vulnerable to directed attacks. Critical bridge nodes connect clusters in the network. Disabling a bridge node disconnects clusters and causes the network to fail. Those bridge nodes are not necessarily in the U.S., but have potentially very large impacts on U.S. trade. The global container shipping system depends on integrated schedules and transshipment ports to function smoothly. Local action disrupting ports that act as bridge nodes can cause effects globally. Disruptions cascade through the system.

Ports are not interchangeable in equipment, physical characteristics or capacity. Forty percent of all marine containers enter the U.S. through Los Angles, one of two post-Panamax[24] container ports on the West Coast. You cannot simply reroute post-Panamax ships to other ports. At any given time, hundreds of ships carry hundreds of thousands of containers loaded by port rotation – all with Los Angeles in the rotation. If L.A. closes, ships will continue to arrive hourly and need someplace to go. There also must be sufficient spare inland transport capacity to clear any diverted containers. If a few post-Panamax ships divert to Tacoma, the other West-Coast post-Panamax port, there might not be rail capacity to move the goods inland. Understanding the global system as a system with interdependencies and network interaction effects is critical to proper policy.

An understanding of international supply chains is critical in developing policy. The costs of protection need to be measured in not just dollars spent but also in the cost of disruption due to protection. Protection should not be more costly than attacks. A GAO report on C-TPAT notes a 2002 Booz Allen Hamilton simulated scenario in which the detonation of weapons smuggled in cargo containers shut down all U.S. seaports for 12 days costing the U.S. economy $58 billion. The pertinent point here is that, in the exercise, the attacks did not close the U.S. seaports. They were closed by government participants in the game in response to attempted but unsuccessful attacks. It is inaccurate to say the bad guys did $58 billion in damage to the U.S. economy. U.S. response to a far smaller failed attack is what did the damage. This also causes us to consider what it means to succeed or fail in this area. The bad guys provoked us into doing $58 billion in damage to ourselves, including disruption to ports and supply chains upon which military activity in Iraq and Afghanistan depends, with no increase in security. Did they fail?

Modern automated ports are an intricate ballet of big machines and 20-ton boxes, all choreographed by computers. If the computers stop working, or data integrity becomes suspect, the terminals stop working. It only takes a talented hacker to disable a container terminal – no need to get anywhere near

23 "A variety of complex systems share an important property: some nodes have a tremendous number of connections to other nodes, whereas most nodes have just a handful. The popular nodes, called hubs, can have hundreds, thousands, or even millions of links. In this sense, the network appears to have no scale." Albert-Laszlo Barabasi and Eric Bonabeau, Scale-Free Networks, Scientific American, May 2003.

24 Panamax ships are the maximum size and draft that can pass through the Panama Canal. Post-Panamax ships are larger than Panamax ships.

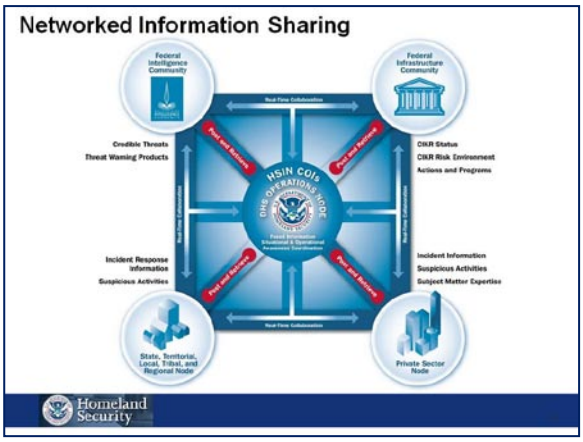
it. If the databases that contain all the information shippers supply under programs such as C-TPAT[25] are compromised, the information is not trustworthy. What happens in terms of inbound container security? Do we stop trade?

There are many examples of these sorts of single points of failure across the global supply chain infrastructure and specifically in the U.S. Significant havoc in the global supply chain can be caused by attacking shore transition points for fiber optic cable where the U.S. plugs into the global information grid. Those points are few and locations well known.

The U.S. interpretation of piracy does not meet reality. In the Horn of Africa, piracy is all they have. Piracy is direct result of a lack of action by the international community to the breakdown of government in Somalia. It has not yet become a systems-level disruption to trade, only an individual ship basis, but that doesn't mean it won't become one at some point. International consensus on how to handle the problem in Somalia is also a part of the problem. Should U.S. policy focus on international piracy or piracy on U.S. flag vessels?

Department of Homeland Security Infrastructure Protection Perspective

Mr. Tom Watson
Director Infrastructure Coordination and Analysis
Office of Infrastructure Protection (OIP)
U.S. Department of Homeland Security
www.dhs.gov/xabout/structure/gc_1185203138955.shtm



One of the missions of the Office of Infrastructure Protection[26] is to form partnerships with industry related to infrastructure. The second National Infrastructure Protection Plan (NIPP)[27] unifies the structure for the government and private sector to improve protection and resiliency of critical infrastructure. OIP used a risk management framework to build the NIPP as an all-hazards homeland security framework. After Katrina, the focus shifted from only terrorism to all hazards.

The goal is to enhance situational awareness and maximize the ability of government and private sector security partners to assess risks, respond to threats, and coordinate programs and processes. OIP seeks to facilitate development and ongoing support of security partner governance and coordination structures. Another aspect of

25 The Customs-Trade Partnership Against Terrorism is a U.S. Customs and Border Protection (CBP) initiative in which businesses ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain. In return for sharing their information, businesses benefit from a more secure global supply chain, a reduced number of CBP inspections, and priority processing for CBP inspections. C-TPAT Supply Chain Security Specialists (SCSS) work with the company to validate and enhance security throughout the company's international supply chain.

26 OIP is the lead for the Maritime Domain Awareness Infrastructure Information Hub. The U.S. National Concept of Operations for Maritime Domain Awareness recommended creating hubs to coordinate the flow of specific types of information while a global maritime information sharing network develops. For more information on MDA Enterprise Hubs, please see Appendix B.

27 The National Infrastructure Protection Plan sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for Federal, State, local, tribal, territorial, and private sector partners. The NIPP provides a coordinated approach that is used to establish national priorities, goals, and requirements for infrastructure protection so that funding and resources are applied in the most effective manner.

improving information sharing is being able to grant security clearances to private sector personnel to expedite disseminating threat information to industry executives. Implementing the CIKR ISE[28] requires finding out what is important to industry. This also includes development of a mechanism for networked information sharing; the goal is to create a seamless process which provides useful information to all customers, delivering critical information where and when it's needed. The framework for this coordinated information sharing is the creation of advisory councils on all levels including infrastructure, sector, government and regional. FACA[29] exemption enables OIP to operate more easily with industry.

NIPP is concerned with both the steady state, and the national incident response framework. The steady state of information flow during normal operating environment includes prevention, preparedness, response, recovery and mitigation. Incident management involves modification of information flow in response to natural emergency or terrorism. With the use of incident management, the situation is divided into three phases: pre-incident, incident and post-incident.

Participant Discussion:

- How is classified information sharing conducted during exercises? Classified information is shared in face-to-face briefings at the ISAC[30], and via secure phone to secure facilities. How is access granted? The Coast Guard can grant access, and the OIP has additional capability to grant it at the Sector Coordinating Council.
- Industry trusts Coast Guard Maritime Security Councils. How does this fit with those? FACA exemptions give OIP flexibility to operate under a different construct and under a different set of rules.

Ship/Port Agents' Perspective

Mr. Jeffrey Milstein
Director of Field Operations
Office of Maritime & Port Security
Moran Shipping Agencies, Inc.
www.moranshipping.com

Ship/Port agents handle 100% of vessel issues from 96-hour notification of arrival to departure and often we are the first face foreign vessels see upon arriving in the U.S. They often board a vessel before Customs and Border Protection or the Coast Guard and may be the first face seen by foreign vessels coming to the U.S. However, ship/port agents are not required by the U.S. government to be licensed and trained, but once hired can be in charge and responsible of the entire security of a port. There

28 Critical Infrastructure and Key Resources (CIKR) Information Sharing Environment (ISE) is being developed under the NIPP. The ultimate goal is to create a nationwide network in which all CIKR partners may effectively collaborate to prepare for, protect against, respond to, and recover from a terrorist attack, national disaster, or other emergency. To enable the protection of CIKR, the Department of Homeland Security established an information-sharing network that is guided primarily by the NIPP and works in coordination with the efforts of the Federal Information Sharing Environment (ISE). For more information, please see http://www.dhs.gov/xlibrary/assets/ NIPP_InfoSharing.pdf.

29 The Federal Advisory Committee Act was enacted in 1972 to ensure that advice by the various advisory committees formed over the years is objective and accessible to the public. The Act formalized a process for establishing, operating, overseeing, and terminating these advisory bodies and created the Committee Management Secretariat to monitor compliance with the Act. For more information, please visit www.gsa.gov.

30 For more on Information Sharing and Analysis Centers (ISAC), please see The Maritime Security Council Perspective, presented by Mr. Will Watson during the first panel discussion, Establishing Efficient Means for Threat Warning Information Exchange between International Maritime Industry & Government.

should be a STCW[31]-type requirement for ship agents. Agents transfer massive funds to international entities with little scrutiny, and have access to vessel itineraries and physical access to port facilities. Ship agents should be incorporated into the TWIC program.

The United States demands a great deal of security cooperation from other nations, but the biggest complaint of foreign shippers is that the U.S. does not reciprocate. GreenLane[32] is probably the most effective program because it has an integrated approach.

The Safety Act of 2002[33] is the most important component of security. The U.S. is currently the only country that does not have a recognized security organization (RSO)[34] or authority to vet "security companies" to ensure quality of services and reliability of service providers. This leads to private companies assuming the role of the RSO. Companies with no understanding of the maritime domain are managing security – they hire a retired Coast Guard officer to sit in the home office and they are suddenly maritime experts. Some ports rely on police officers for security – they have no understanding of maritime but are authorized to use deadly force. Companies spend millions on systems and pay $6 an hour to man them. TWIC is too easy to get, so it is meaningless.

The U.S. government needs to upgrade MTSA[35] to pressure International Maritime Organization (IMO) to upgrade ISPS.

A minimum understanding of the maritime community by maritime/port security guards is needed to provide adequate security. Vessel security and smooth operations can be in conflict, so there should be a feedback mechanism where these conflicts and be resolved. Furthermore, the Vessel Security Officer (VSO) should not be a collateral duty. It is often a tertiary duty and they are overloaded. Vessel security

---

31 The International Convention for Standards of Training, Certification & Watchkeeping (STCW), adopted in 1978 by conference at the International Maritime Organization (IMO) in London, entered into force in 1984, and significantly amended in 1995, sets qualification standards for masters, officers and watch personnel on seagoing merchant ships.

32 The GreenLane Maritime Cargo Security bill was authored by Senator Patty Murray (D-WA) and introduced with Senator Susan Collins (R-ME) in 2005. It was revised to include provisions from the Public Transportation Terrorism Prevention Act and enacted as the Port Security Improvement Act of 2006. It is a companion piece to the Security and Accountability of Every (SAFE) Port Act, introduced in the House of Representatives in by Representative Dan Lungren (R-CA) and Representative Jane Harman (D-CA). The Port Security Improvement Act raised security standards for all cargo entering the U.S., created a "GreenLane" to track and monitor cargo, created a system to resume trade after an incident, and funded port security grants. The Port Security Improvement Act also strengthened the Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT) programs codified by the SAFE Port Act.

33 The goal of the SAFETY Act is to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability protections. In 2008, the U.S. Office of Management and Budget performed an evaluation of the Office of SAFETY Act Implementation (OSAI), using its Program Assessment Rating Tool (PART). OSAI earned a score of Effective, the highest rating a program can achieve. According to OMB, programs rated Effective set ambitious goals, achieve results, are well-managed and improve efficiency. OSAI was one of only 10 programs in DHS to receive a score of Effective (61 DHS programs were evaluated). See www.safetyact.org.

34 Recognized Security Organization, under the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code. The ISPS Code is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The ISPS Code is implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS). The Code has two parts, one mandatory and one recommendatory. In essence, the Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. The purpose of the Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures. Under the provisions of SOLAS regulation I/6 and, inter alia, SOLAS regulation XI-2/1.16, Special measures to enhance maritime security., Recognized Security Organizations (RSOs) may be delegated specific functions on behalf of the Administration and/or the Designated Authority of the Contracting Government, including: approval of ships security plans; verification for ships issuance and endorsement of International Ship Security Certificates; and development of port facility security assessments. See www.imo.org.

35 The Maritime Transportation Security Act of 2002 is essentially the U.S. domestic counterpart to the ISPS Code.

and smooth operations can be in conflict: a feedback mechanism is required to resolve conflicts. An network of legitimate VSOs would establish effective information sharing with each other and the government.

Security lapses also exist in gate lists to the port facilities; currently, there is no vetting of gate lists and no established security scanning on who gets on the vessels. Chandlers abuse the system to sell to the ship – how many other people are getting around the system? There is also little inspection of ship deliveries, e.g. packages that are allowed on the ship. The only industry that is inspecting packages is cruise ships because their commodity is passengers.

There is too much focus on containers while other threat areas are ignored. It would be easy to hide weapons in false pipes in an engine room and Coast Guard inspectors would never find them. Petroleum tankers are hard to track because they are trampers.

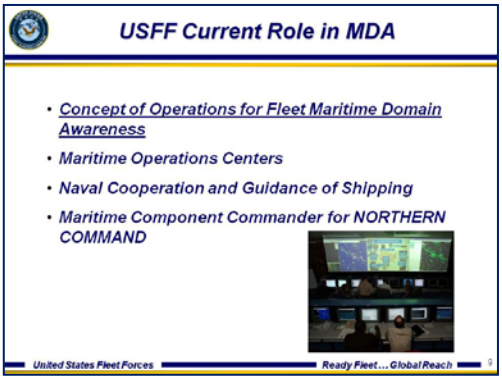
Ship agents are MDA by definition. They should be incorporated more fully into plans to achieve MDA.

Industry–Government Dialog – Digging Deeper

MDA for America and Beyond

Rear Admiral Dennis FitzPatrick, USN
N3 Joint Operations Director
U.S. Fleet Forces Command
U.S. Navy
www.cffc.navy.mil/

The Cooperative Strategy for 21st Century Seapower is a revision of U.S. Navy's maritime strategy connecting U.S. Navy, U.S. Marine Corps and U.S. Coast Guard; the strategy is also endorsed by all three services. Preventing wars is as important as winning wars. Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy or environment of the U.S. Maritime Security Operations include anti-piracy measures. Humanitarian assistance includes cooperation with non-government organizations.



The U.S. Navy (USN) seeks MDA through organic assets as well as by global information sharing partnerships. Furthermore, USN recognizes the need for sharing of unclassified information across government agencies as well as to the private sector. U.S. Fleet Forces' current role in MDA is through Maritime Operations Centers and through NCAGS (Naval Cooperation and Guidance for Shipping) units. Maritime Operation Centers are regional offices that coordinate information resources.

Future challenges in implementing MDA are that information sharing needs to move to a low-tech level that is unclassified and accessible. Furthermore, organizations within USN, USMC, USCG need to integrate the MDA subject matter experts so that information can flow freely within the government and to the private sector.

Participant Discussion:

- How can foreign navies, e.g. Singapore, build relationships with the U.S. Navy to share information on MDA? Work with the regional MDA offices within the service, and the regional Combatant Commanders.
- Is U.S. Southern Command's Enduring Friendship Program as an example of a partnership? The Enduring Friendship program uses combatant ships and transforms them to be medical ships, which provide services to a local population with the partnership of the local country after a disaster. Mostly, these ships are offering humanitarian care to the poor of that country. While the local people were extremely happy and satisfied with the care, the local government was not. This feedback was used to make sure we are partnering with the local governments on these humanitarian missions. And perhaps most importantly is the enduring aspect of this mission; we need to make sure we are coming back again. We cannot show up once. Rather, we need to continually visit to form and build this hopefully lasting relationship.
- Who is in charge of MDA? This is a follow-up to the question asked to others on Day One. The U.S. Navy is *not* unilaterally taking over. MDA requires a collaborative approach.

An Industry Perspective on Piracy

Mr. Phillip J. Shapiro
President & CEO
Liberty Maritime Corporation
www.libertymar.com

The Liberty Sun, a U.S. flagged cargo ship was attacked April 14, 2009[36]. However, the pirates failed to board the ship. The attack was two days after the rescue of Captain Phillips of the Maersk Alabama (and was seen as a retaliation to the pirates who were killed). The ship was on a humanitarian aid mission heading to Kenya and Somalia. Thankfully, no one on aboard the Liberty Sun was hurt and the captain followed the security plan that was designated by Liberty Maritime Corporation.

The recent incidents of pirate attacks against U.S. flagged ships and non-U.S. flagged ships has forced the Department of State (DOS) to examine current policy dealing with piracy. Many companies have complained that getting assistance from the U.S. government either during or since an attack has been more difficult than dealing with the attack itself. Furthermore, these attacks have raised the controversial issue of whether ship owners should carry firearms on ships in order to protect the crew and cargo.

There are restrictions to carrying firearms on a ship as most foreign governments do not allow ships with firearms aboard into their ports. If they do allow the ship into port, typically a license is required at a significant fee – sometimes up to $15,000/month. In response to the piracy, Congress and DOS has asked the U.S. Navy to protect ships traveling through the Horn of Africa and Gulf of Aden by adopting the Cummings Amendment[37]. The Navy, however, argues it is already stretched too thin and does not

36 For more information on the attack, please visit http://edition.cnn.com/2009/WORLD/africa/04/14/somalia.pirates/index.html.

37 Congressman Elijah E. Cummings (D-Md.), Chairman of the House Subcommittee on Coast Guard and Maritime Transportation, introduced an amendment to the 2009 Defense Authorization Bill that that would require the U.S. Department of Defense to protect U.S.-flagged ships at risk of being boarded by pirates under the rational that not doing so is analogous to leaving U.S. soil unguarded if it faces the risk of attack. The amendment was not included in the 2009 Defense Authorization Act. Instead, the act included the requirement that the Secretary of Defense and the Secretary of State submit a report to Congress within 60 days after enactment, setting forth what actions the Departments have taken to: eliminate or reduce restrictions under any regulation or provision of law on the carriage of arms and use of armed security teams on United States-flagged commercial vessels for purpose of self-defense; negotiate bilateral agreements to permit U.S.-flag vessels to enter foreign ports while carrying fire arms for self protection; and establish common standards for the training and professional qualifications of armed security teams.

have the resources to escort every U.S. flagged ship through these areas. Additionally, this amendment only protects U.S. flagged ships, which are a minority on the seas; many U.S. companies have ships flagged by other countries and those ships would not be protected under the Cummings Amendment.

Meanwhile, the State Department has begun negotiations with the countries located in East Africa regarding their fees and port regulations in regards to firearms, but these negotiations will take time.

U.S. State Department Counter-Piracy Perspective

Mr. Andrew Shapiro
Assistant Secretary of State for Political-Military Affairs
U.S. Department of State
www.state.gov/t/pm/

Each year 33,000 ships pass through the Gulf of Aden. In the first nine months of 2009, piracy attacks have already exceeded 140 and are increasing in areas such as the Indian Ocean and Red Sea. The Department of State believes piracy attacks have increased because the Somali government has not created a stable economy and government system in that country. And efforts to work with the government of Somalia to prevent piracy along their coast are not yielding immediate results.

DoS's policy on piracy attacks is that our government will not provide ransoms and will prosecute pirates in international courts. For example, the decision to prosecute the pirate captured in the Maersk Alabama attack shows our dedication to prosecuting these criminals. An international trust fund has been created to help prosecute the pirates and the United Nations will administrate the fund (.92 of every $1 will go to the fund). Furthermore, witnesses need to be encouraged to testify and shipping companies need support the prosecution.

Currently, our government is searching for ways to disrupt the flow of money between pirates and their handlers. We need to better understand the financing activities and need to be able to disrupt these activities. In order to combat piracy, there needs to be cooperation between international nations and private industry when it comes to sharing information and prosecuting the criminals.

Voyage Risk Assessment

Mr. Giles Noakes
Chief Maritime Security Officer
Baltic & International Maritime Council (BIMCO)
www.bimco.org

Industry is cooperating with government to prevent piracy. Illegal maritime activities are threats to global trade. BIMCO lobbies on behalf of the industry. Currently, piracy is only one of many challenges the maritime industry is facing; others include port security and cargo security scanning. BIMCO supports ISPS Code as the bible for the shipping industry.

In order to ensure sharing of information, BIMCO advocates that the culture of classifying MDA information needs to be eliminated. Furthermore, merchant mariners need to be educated on anti-piracy best practices. Insurance companies are an important stakeholder in anti-piracy.

The Internet is the best resource for port-specific threat assessment. BIMCO has promulgated risk assessment measures and threat mitigators. BIMCO has an online questionnaire and will provide a

threat score for a given vessel in a given port (for a fee). AVRA[38] provides risk assessment for vessel owners.

Participant Discussion:

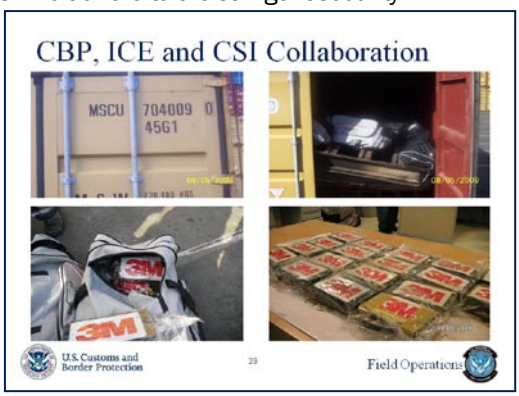
- Regarding arming merchant crews, SOLAS governs liability on merchant ships. It does not address arming the crew. The ship-owner's liability for armed conflict incidents is too great for arming crewmembers.
- The global legal system is failing to prosecute pirates. 51.75% of suspects arrested for piracy are being released, often after being caught in the act.

Customs & Border Protection Perspective

Mr. Frank Jaramillo
Director
National Targeting Center (Cargo)
U.S. Customs and Border Protection (CBP)
U.S. Department of Homeland Security
www.cbp.gov

The mission of Customs and Border Protection is as the guardians of our Nation's borders – America's frontline: to safeguard the public against terrorism. The National Targeting Center's mission is a critical component in CBP's layered enforcement strategy; it's international in scope. It is the goal of the National Targeting Center – Cargo (NTC-C)[39] to proactively target and coordinate examinations of high-risk cargo in all modes of transport. Cargo control is one aspect of border patrol. All cargo must be laden 24 hours prior to loading. The majority of cargo bound for the U.S. is inspected in foreign ports by radiological screening, container inspection, etc.

With the creation of the Customs and Trade Partnership Against Terrorism (C-TPAT), CBP is attempting to provide an incentive to industry partners by providing streamlined procedures for partners who demonstrate sustained stringent reporting. Those suppliers who adhere to the stringent security measures should be given reduced inspections at port of entry. To date, the total number of certified members is 9,439.



In December 2006, the Department of Homeland Security, as part of the efforts to meet the requirements of the Security and Accountability For Every Port Act of 2006, known as the SAFE Port Act, created the Transportation Worker Identification Credential (TWIC) program and establishment of interagency operational centers for port security.

38 BIMCO's Automated Vessel Risk Assessment (AVRA) service is a web-based threat-assessment system with a risk engine that generates individual threat assessments for an individual vessel making an individual voyage.

39 NTC-C is the lead for the Maritime Domain Awareness Cargo Information Hub. The National Targeting Center – People (NTC-P) is the lead for the Maritime Domain Awareness People Information Hub. The U.S. National Concept of Operations for Maritime Domain Awareness recommended creating hubs to coordinate the flow of specific types of information while a global maritime information sharing network develops. For more information on MDA Enterprise Hubs, please see Appendix B.

Furthermore, the DHS developed partnerships with the Department of Energy, Department of State, foreign governments and the trade community; all are involved in the program to scan cargo virtually, which would be analyzed at the NTC center in Herndon VA. Ports where virtual scanning exists are ports that are at high risk.

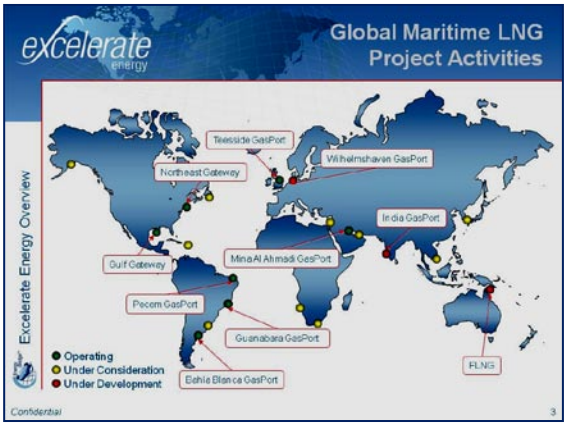
Participant Discussion:

- Is there a way companies can get a list of companies that are on the DHS watch list so that they can better police their shipments? DHS lists include suspected companies. Government must be careful not to put legitimate companies out of business by providing a watch list without evidence to support wrongdoing.
- Regarding oil tanker tracking movements and the extra paperwork that has to be filed to track movements – the Automated Manifest System is an archaic system. AMS with regard to oil tankers: it requires considerable administrative support for diverted oil tankers. Why so much focus on the tramp trades? Breakbulk and bulk cargo pose a risk. The tracking process is being modernized to use the new systems in place for container ships to support general cargo vessels.
- Does CBP verify the last five ports of call? Does Border Patrol harmonize passenger lists with Coast Guard? USCG and CBP harmonize lists. Government wants a strong flow of information for better response. Also, last ports of call are checked against records.
- How do you analyze risk on empty containers? CBP looks at last port of call, movement of the container and the original location. Overall, CBP looks at very few empty containers.

LNG Shipping Perspective

Captain Mark Lane
Senior VP Operations
Excelerate Energy, LLC
www.excelerateenergy.com

There have been a few disasters over the years involving Liquefied Natural Gas in 1917, 1944, 1964, 1969 and 1973. Each incident provides new impetus for modernization. Currently there are two types of design – ball-type and membrane-type cargo carriers. The potential for disaster with LNG is higher than with a number of other types of product, so risk management is more stringent. The LNG fleet is growing at an exponential rate and the safety record is impressive. To date there has been no loss of life and no spillage of cargo.



The risk of piracy attacks is minimal with LNG carriers because they are more difficult to board. There is still the risk because LNG ships could possibly be used as weapons of mass destruction if modifications to control systems and cargo were able to be accomplished. Threat assessment of world LNG terminals is also an aspect of the companies' risk management. Each terminal has some vulnerability and measures are in place to mitigate each threat. There is a move to offshore facilities for liquefaction and storage in order to reduce the threat to land terminals.

Panel Discussions

First Panel:
"Establishing Efficient Means for Threat Warning Information Exchange between international Maritime industry and Governments"

Panel Moderator
Mr. Owen Doherty
Director, Office of Security
U.S. Maritime Administration
U.S. Department of Transportation
www.marad.dot.gov

MARAD is not a security provider, but we represent the interests of the industry. MARAD wants to play a role in improving information sharing between federal, state, local government and private industry, and this panel's purpose is to explore those relationships.

Benchmarking Partners Perspective

Mr. Ted Rybeck
Chief Excutive Officer
Benchmarking Partners
www.benchmarking.com

Maritime Security is bureaucratically complex; technology is easier and needs to be widely accepted within the maritime industry. Furthermore, younger intelligence analysts prefer the 99% open source to the 1% from intelligence sources. The intelligence community bunkered in and doesn't have access to most of what bad guys and 16-year-olds get. For example, leaving your cell phone at the door of the secure facility protects you from the less likely threats and cuts you off from the flood of data on the more likely threats. There is great benefit in the use of multiple technologies and applications together for intelligence analysis – for example mashups[40] using Google maps and radiological activity sensors.

We make irrational decisions during crises that don't hold up to cold analysis

A demonstration of interagency involvement is required for a positive outcome to the terrorist threat. The technology can be managed with free stuff available to most 16-year-olds. The new federal CIO is putting out billions of data points open source through mashups. The information is readily available so the question is, how well will be use it? The Fed CIO use to work for the city of Washington DC. There is more information available on auto theft in DC[41] than you are getting on the entire maritime domain. While change does not need to dramatic, it does need to be timely. Compare what's been accomplished since 9/11 to the time it took to fight WWII.

40 Mashups, also called Web Application Hybrids, are Web pages or applications that merge the functionality and/or data from multiple sources to create a new service. An example is the International Chamber of Commerce Commercial Crime Services Live Piracy Map at available at www.icc-ccs.org.

41 See http://crimemap.dc.gov/presentation/query.asp

Maritime Security Council Perspective

Mr. William Watson
Board of Governors
Maritime Security Council
www.maritimesecurity.org

The Maritime Security Council was established in 1988 and represents all branches of the maritime industry. It works with governmental and industry groups internationally. The best method to exchange information is a key initiative for MSC. MCS advocates the best method to exchange information is to develop an Information Sharing and Analysis Center (ISAC)[42]. There are 12 ISACs that share two traits: they are resourced by government and overseen by industry. Only in the maritime sector is the government determined to control information sharing directly. However, there is a fear of sharing with the Coast Guard information that could be useful to many others because it could result in a security inspection by the Coast Guard that would cost money and efficiency.

It has been suggested that the maritime sector could piggy-back on another ISAC. That fails to recognize the unique nature of the maritime industry. An independent Maritime ISAC is the only way to share information between sectors, and internationally. Information sharing is only effective if conducted with all parties that need to know. The U.S. federal government should endorse and fund an independent ISAC. The MSC fully supports its establishment.

Industry Perspective

Mr. Eric Ebeling
Director of Government Relations
American Shipping and Logistics Group
www.amslgroup.com

For maritime information sharing, at best the government is translucent, but more often opaque because of the multiple layers of bureaucracy. The biggest obstacle is the lack of a single reporting 911 system. There are currently too many cooks in the kitchen. OSAC[43] is a good model of what works right. The GMISS conference is a good example of progress when it comes to information sharing, particularly rolling multiple conferences into one. Often the government (federal, state, and local) require transparency of private sector, but do not relay what is being done with that information.

The U.S. Flagged fleet is the most cost effective option available to U.S. government and is eight to ten times more cost effective than a government owned and operated fleet.

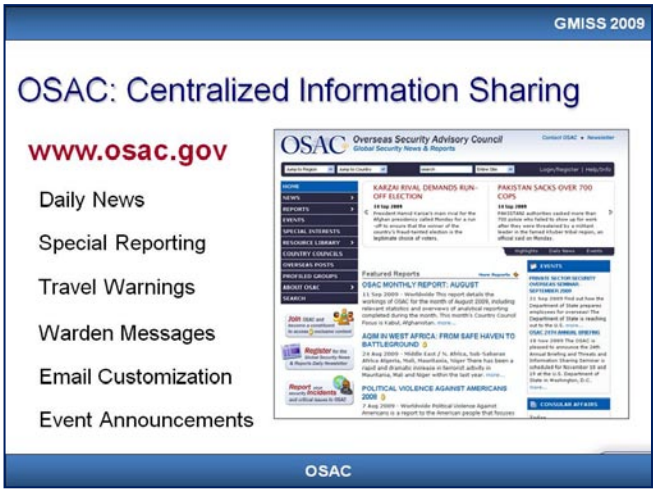
---

42 ISACs were established under Presidential Decision Directive 63 (PDD-63) in 1998. The directive emphasized that, because 90% of the nation's critical infrastructures are owned and operated by the private sector, a public and private partnership is needed to share information about physical and cyber threats, vulnerabilities, and incidents to help protect the critical infrastructures of the United States. PDD-63 was updated in 2003 with Homeland Security Presidential Directive/HSPD-7 to reaffirm the partnership mission. ISACs are trusted entities established by critical infrastructure owners and operators. The ISACs have unique capabilities to provide comprehensive sector analysis and have the ability to reach extensively within their sectors, with other sectors, and with government to share critical information. The ISACs respond to all aspects of security and "all hazards." For example, ISACs have been established for: Communications, the Electricity Sector, Financial Services, Information Technology, Surface Transportation, Public Transit, and Water. The ISAC Council establishes and maintains a framework for interaction between and among the ISACs and with government. In 2007, the Maritime Security Council (MSC) became the first maritime industry member of the ISAC Council where it promotes the exchange of information and intelligence within the maritime industry and with other critical infrastructures. A Maritime ISAC is chartered under the ISAC Council, however there has been limited industry interest in participation. Please see www.isaccouncil.org for more information.

43 The U.S. Department of State's Overseas Security Advisory Council. Please see The OSAC Perspective by Mr. Mike Limpantsis immediately following.

Overseas Security Advisory Council (OSAC) Perspective

Mr. Mike Limpantsis
Acting Director
Overseas Security Advisory Council (OSAC)
U.S. Department of State
www.osac.gov



The Overseas Security Council was created in 1985 with the original mission to protect U.S. businesses overseas. OSAC is a public private venture to promote security cooperation between the private sector worldwide and U.S. government. Today it is a joint venture with a current constituency of 6,000 private sector organizations and over 120 local OSAC country councils.

OSAC provides centralized information sharing via our website, www.osac.gov. We streamline and declassify information in order for this information to be disseminated to a wider audience. Where stakeholders face common challenges and threats, we find collaboration replaces proprietary concerns. We're trying to find those commonalities in our maritime outreach. We push and pull information we get info from private sector, scrub it, and put it back out in ways that protect provider but also so others can use it. Furthermore our country councils enable us to break down local barriers so that information is more accessible to all users. We are looking for feedback from you, both private and public sector, to improve our system of information sharing. Tell us how to get the information out across borders in the international spectrum.

DHS Intelligence Perspective

Rear Adm. James B. Plehal, USN, (Retired)
Senior Advisor – Intelligence
Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
www.dhs.gov/xabout/structure/editorial_0794.shtm

There have been significant changes in the way we do things since 9/11. While information sharing has much work to do, it is moving in the right direction because of meetings like this. The concepts discussed at GMISS should translate into individual projects that can be tracked and accomplished. Getting the private and public sectors in a room to work things out together is a lot of progress. All participants – government, military and private sector – need to be speaking the same language.

The intel community cannot connect the dots until it has the dots. Getting the dots has traditionally been the intel community's job, but that is expanding. We have to figure out what dots we actually need: to clarify the requirements, which requires a lot of dialog. Federal government agencies, beyond intelligence agencies, are working together on these tasks with state, local and tribal communities. All of

these players are needed to connect the intelligence dots and disseminate it to the maritime industry. As far as dissemination, how do you vet the people? Who do you disseminate to? Traditionally that has been federal, but how do you expand that without stepping civil rights and civil liberties?

Participant Discussion:

- Currently, OSAC information is country specific – but cities in same nation can be completely different. Can OSAC add another tier? In the new website, you will be able to break down to the new information, by region and city. It will be available in the summer of 2010. For example, we have five councils in India covering each major city in its region.
- Is the panel aware of the Southeast Asia/Africa (Indian Ocean) Cooperative? There is a strong desire to better engage with industry. The organizers brought in OGMSA to help coordinate. It is seeking cooperation across the Indian Ocean for maritime security. Looking to network and engage with this region. One of the goals is to bring industry issues in front of international bodies. Looking for opportunities to engage with ship owners, industry, etc – meet with the ministries and port authority in these countries. Furthermore, the cooperative took six goals of this symposium – and they agreed yes, this is the same thing they want to accomplish.
- How can government put out classified info so it's usable? It's easy to de-classify material (example Iraq) – and for non-classified actors to use the information. The problem arises when the non-classified actors build information of their own and the government wants to use it – in a classified form. The way forward was about two sets of architecture: one with open information sharing, the other for intelligence that doesn't involve industry, unless it is so big it needs to be declassified and disseminated.
- An unclassified network is most commonly used, and the government should be able to share this information as quickly as possible, ideally on the cell phones at the speed of Twitter[44]. What part of the U.S. government is willing to host this information center, and what part should pay for it? What specific information is desired determines which agency provides the data under current constructs. The government wants information that is vetted and true to go out, not necessarily a ticker of raw Twitter feeds. You need information you can trust. One of the reasons OSAC information is so important is that it is vetted and can be trusted. The danger of instant information is that it is hard to make it accurate. There is a risk of information overload if all data is pushed through in a Twitter-like format. If it is done by the intelligence community, there is an inherent problem regarding turf issues, etcetera. The Government Services Agency (GSA) could provide the service through dot-gov capabilities. GSA for government can be tied into the private sector using Wikipedia technology. It can incorporate peer-produced linking. You can merge these systems: GSA, Intellipedia, private sector systems that already exist, fed by Twitter.
- ODNI is trying to share threat information with people on the waterfront, but is looking for a focal point. The state fusion centers look like a focal point. Keep in mind sovereignty issues. Dealing with industry in the state of California, there's a state government with authority, so federal authority is in question. We would hope local representatives know better than we do who the points of contact are. MIST is developing this better. It is a very complex issue. In the private sector, it's possible I don't need to know what the specific intel is, just what I need to do to protect assets. I already get info by text on my cell phone. I got Mumbai information from OSAC before CNN. I do need to trust the source. Then tell me what to do.

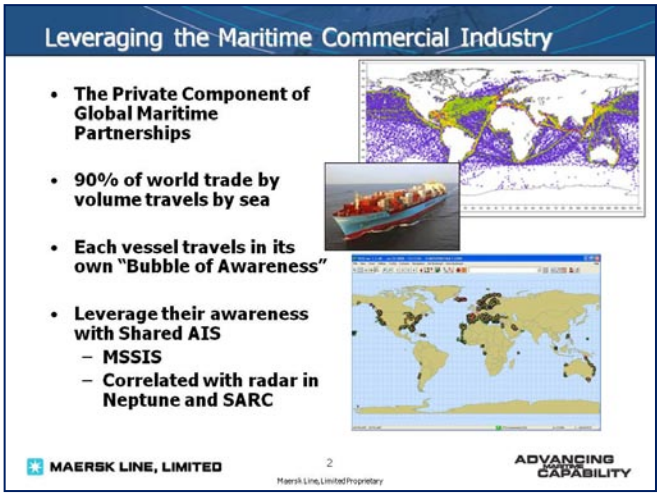
44 Twitter is a free Internet-based service that enables its users to send and read text-based messages of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers via the Twitter Website, Short Message Service (SMS) texts on their cell phones and mobile devices, or other external applications. Senders can restrict delivery to those in a specific group or, by default, allow open access.

Participant Discussion:

- These issues have been percolating without resolution for some time now, which is the source of frustration in this room. How does the information get from this incredible bureaucracy to the guy who needs to make a decision this morning about how to deploy resources? That has to translate down quickly to enable him to make adjustments. All of these comments link together. It isn't technology. It's about getting the information from the people who have it to those who will use it immediately. Can my ship go through the channel? What do I tell my marine patrol guys to look for today? Government realizes that's the goal. It's easy to find an example that makes it seem clear cut. Government struggles with knowing how industry really operates and what industry really does need, but also, when do I get you out of bed and say, "This is an issue?" That information doesn't come along very often.
- The world has shifted. Local police did not immediately blast information out to the public. That has changed. If you have an issue, you're putting it out early and often. Think: Virginia Tech. We have to get the information out sooner. There's a lot of operational information that must come out very quickly – Mumbai – information there that could have come out quickly – methods, comms, etc, that we would like to have been able to keep our eyes open for immediately so we could do something about it. The world has accelerated. That needs to tie into this discussion. The point was made that you need to wait until information has been vetted. But if you put out the basic facts that you do have, all of a sudden private sector people on site can feed information back as it develops. Don't hold the information until you figure it out. Get something out there and let local experts help develop the picture. The Amber Alert model is useful. Once the information has been reported and information has been shared, the people on scene are empowered to help take away an emerging threat. Inside the beltway, there doesn't seem to be the same kind of political will you see with the Amber Alert program.
- Government doesn't have a clear understanding of how the industry works. When there was an incident on a facility, the facility owner didn't know what agencies were coming in. There was a total lack of coordination. Longshoremen stop work, which creates health and safety issues. You have to coordinate and work with the port. The last thing we need to do is stop operations for a minor problem. Don't just come in and muscle your way through. Who takes the lead on information sharing – federal or state agencies? State and local authorities have better working relationships with end users. Intelligence is not essential – guidance on evolving precautions can be sufficient.
- Wikipedia is open source information sharing which is competitive with government provided information systems. Real time information on threats during London and Mumbai bombings was being updated rapidly and in real time on Wikipedia. The source is available, but not incorporated into the current MDA environment.
- The Naval Postgraduate School is developing a Maritime Security Certification Course and wants you to help capture these ideas.

Second Panel:
"Industry and Government issues and concerns with Maritime Information Sharing"

Panel Moderator
Capt. Gordon Van Hook, USN (Retired)
Senior Director, Innovation and Concept Development
Maersk Line, Limited
www.maersklinelimited.com



Currently, 90% of the world trade by volume travels by sea and each vessel travels in its own bubble of awareness with little interaction with other vessels and regional maritime centers. The Thousand Ship Navy, now Global Maritime Partnerships, is supposed to include the maritime industry. The maritime industry needs to expand and improve the current awareness systems. They can leverage their awareness with shared AIS systems. Within systems such as MSSIS[45], that data should be correlated with radar, as it is in systems such as Neptune[46] and SARCR[47]. AIS is easy to spoof and alter. It should be treated as one fallable piece of data. If maritime security forces could correlate AIS with vessel radar data, thousands of contacts outside shore-based AIS would be revealed, as well as many anomalies. This has immediate security application in areas such as the Gulf of Aden. SARCR is the next step in exercising these capabilities. These should not be viewed as intelligence systems. They are safety systems.

Begin with commercially flagged vessels of NATO and EU nations and start at the regional level in the Mediterranean Sea. It is already well-served by MSSIS. MSSIS is a successful model and could be used as a base from which to expand.

Can the New York Declaration[48] be expanded? Maritime Security Consortiums are a new kind of public/private partnership. Shared data combined with Maritime Security Consortiums bring great potential. Maritime consortiums start regionally and can work through Maritime Operations Centers to provide expanded analysis. They form the foundation of a maritime community watch. Commercial incentives to participate could include tax breaks, compliance in exchange for further incentives, or as a prerequisite to Jones Act[49] certification.

---

45 The Maritime Safety and Security Information System (MSSIS) is a freely-shared, unclassified, near real-time data collection and distribution network connecting government maritime agencies globally. Its 63 member countries share data from Automatic Identification Systems (AIS), coastal radar, and other maritime-related systems. MSSIS is intended to promote multilateral collaboration and data-sharing among international participants, with a primary goal of increasing maritime security and safety. Data sources may range from a single sensor to an entire national vessel tracking network. Because the data distributed by MSSIS maintains its original, internationally-recognized format and is delivered to users in near real time, member organizations are able to use the feed to meet their own specific mission requirements. Source: Volpe National Transportation Systems Center, Research and Innovative Technology Administration, U.S. Department of Transportation. www.volpe.dot.gov.

46 Neptune is a data fusion system developed by Lockheed Martin that combines the data from a ship's radar and its AIS transponder and uploads it to a fusion center. Beginning in 2006, the U.S. Department of Transportation funded a test project that placed Neptune on Maersk Line Limited vessels.

47 The Shipboard AIS and Radar Contact Reporting (SARCR) project is a DHS initiative to fuse shipboard AIS and radar data and upload it to government fusion centers. Initiated by Mr. Guy Thomas, OGMSA's Science and Technology Advisor, SARC was successfully tested aboard one U.S. flagged commercial vessel during 2009 and agreements are in place to expand to six cargo vessels and a cruise ship.

48 The New York Declaration is a commitment to best management practices and adherence to the ISPS Code to avoid, deter or delay acts of piracy. Representatives from the United States, Japan, the Republic of Cyprus, the Republic of Singapore, and the United Kingdom of Great Britain and Northern Ireland signed the New York Declaration on the eve of the Fourth Plenary Session of the Contact Group on Piracy off the Coast of Somalia at United Nations Headquarters in New York on September 10, 2009. The original signers of the declaration on May 29, 2009 were the Commonwealth of the Bahamas, the Republic of Liberia, the Republic of the Marshall Islands, and the Republic of Panama. Source: U.S. Department of State, www.dos.gov.

49 The Merchant Marine Act of 1920, sponsored by Senator Wesley L. Jones of Washington, is widely known as the Jones Act. It governs compensation rights of sailors and requires, essentially, that all commerce conducted by water between U.S. ports is reserved for vessels that are U.S. built, U.S. owned, registered under U.S. law, and U.S. manned.

Port/Maritime Security/Law Enforcement Perspective

Chief Michael Berkow
Chief of Police
Savannah-Chatham Metropolitan Police Department
www.savannahpd.org

I'm addressing the real world in Savannah as Chief of Metropolitan Police Department. Savanna is an inland port city, the fastest growing container port in company, serving about four thousand commercial ships annually. It is one of two LNG ports in an urban area. Police patrol the intercostals waterways and harbor on a daily basis.

What I see happening is the opposite of the theme of this conference – increasing fragmenting of intelligence and increasing federalization. It seems like MDA is being broken apart as opposed to the centralized MDA reporting and dissemination we all want to see. Emergency operations centers call me asking what's really going on on the ground.

I hear people talking about a single 911 call center – that's the National Response Center, originated for pollution, co-opted after 9/11. You call in and hours later you may get something trickling back down. People don't actually call the National Response Center – they call 911 and a dispatcher sends police. We have separated intel from the boots on the ground, which is usually police. In the 60's, we started consolidating police, fire and EMS. It was hugely powerful. Merge that with your focus point and you become better integrated, instead of fragmenting things further. Agencies that should be my partner are building new separate facilities rather than creating synergy.

With brick and mortar command centers, we're not building for the future. We're building Blockbuster video stores. People get their video over the Internet. We need virtual watch centers.

Watching what we're doing with MDA, I find myself flashing back to the efforts to combat drugs, then terrorism. Great sharing centers were built for one issue – drugs. Then, we didn't add terrorism to the anti-drug centers. We built new silos. Why build an MDA silo? Build onto what already exists.

Intelligence Perspective

Mr. Alexander W. Joel
Civil Liberties Protection Officer
U.S. Office of the Director of National Intelligence (ODNI)
www.dni.gov

Fusion Centers on the state levels have brought about questions from citizens regarding the security of the information that is gathered. The Department of Justice initiated the Suspicious Activity Reporting Initiative (SAR), which standardizes reporting and protects civil liberties. The intelligence community and DoJ have been forward-leaning in working with state and local law enforcement as part of the SAR.

The perception from our international counterparts is that the U.S. is the Wild West when it comes to monitoring and surveillance – no rules. The reality is a massive set of rules, which are different for each federal agency, each state, and private sector. It's not the absence of rules – it's the proliferation of them that seems to lead to confusion.

Civil libertarians are uncomfortable with balance metaphor we often hear, with national security on one side, civil liberties/privacy on the other. More of one means less of the other – zero sum game. This is

not necessarily true: securing the data better is beneficial for all parties. We have a set of criteria and controls for each risk we identify.

Project Seahawk Center Perspective

Mr. Frank Guiterrez
Former Deputy Director
Project Seahawk Taskforce
U.S. Department of Justice
www.justice.gov

Before OGMSA and GMAII, before the Department of Homeland Security established as an agency, Project Seahawk was established as a Congressionally funded pilot project. Project Seahawk was the first initiative after 9/11 to enhance Maritime Security, set up under the Department of Justice to look at many of the issues we're looking at here today.

Seahawk involved 15 full-time agencies, federal, state and local, incorporating police and the National Guard. The program paid for the extra law enforcement it required because local law enforcement doesn't have the extra resources to contribute.

Seahawk is still evolving to better interact with newer resources like fusion centers, which perform the intelligence work. Seahawk is an operations center. All assets belong to the contributing organizations, but are tasked as part of a task force toward a common end – the last defense and the first responders.

The next phase of the program is the Interagency Operations Centers (IOC)[50], which launch in October 2009. The IOCs will operate under DHS rather than DoJ. The IOCs will collaborate with the State Fusion Centers for intelligence information sharing. Operations centers don't need a strong understanding of what's going on in Pakistan, for example. Instead, they need a general strategic understanding and specific indicators to be aware of.

(Note: On October 1, 2009 Seahawk moved from the Department of Justice to the Coast Guard on behalf of the Department of Homeland Security)

Chamber of Shipping (UK) Perspective

Mr. Gavin Simmons
Shipping Defence Advisory Committee,
The Chamber of Shipping
www.british-shipping.org

The Shipping Defence Advisory Committee (SDAC) was created in 1937 as a liaison between the shipping industry and government. Project Camelot was launched with the desire to share shipping industry knowledge with the military. It started with six vessels as a voluntary initiative to share information in 2006 and now tracks approximately 600 ships using a maritime data exchange portal.

50 The Interagency Operations Centers/Command 21 (IOC/C21) project was initiated in response to the requirements of the Security and Accountability for Every (SAFE) Port Act of 2006. It is being implemented by the Coast Guard and will transform Sector Command Centers into IOCs by improving facilities, information management, and sensor capabilities. The goal of the IOC/C21 is to improve situational awareness by automating the data fusion, dissemination and anomaly detection processes to close significant gaps in the Coast Guard's ability to see, understand, and share tactical information critical to security and interagency coordination in vulnerable port and coastal areas. Maritime security transportation operations will be coordinated across various levels of government in one location. Source: U.S. Coast Guard, ww.uscg.mil/acquisition/ioc/.

For all ships UK flagged ships and incidents in which they can be involved, there is a range of government agencies involved. Camelot developed a matrix, including who should lead for different types of data. The rules and policy are constantly evolving: we tend to stay about one step ahead.

We cooperate with the IMO, NATO, EU Security and Defense Policy[51], Chiefs of European Navies; Maritime Analysis and Operations Center - Narcotics[52]. The methodology is to create partnerships with private, national and international entities. Success is based on confidence-building between partners, a simple cost structure, an inclusive approach, flag blindness, recognizing all UK shipping interests, and complementary approaches to other interests. Looking forward, the Shipping Defence Advisory Committee and Project Camelot are looking to maintain linkage with other security agencies.

Participant Discussion:

- Does the Shipping Defence Advisory Committee share information with the U.S. government? SCAC does, and has been care careful to avoid the paper bulkheads that exist elsewhere.
- Is there a difference between LRIT (Long Range Identification and Tracking) and AIS (Automatic Identification System)? Is one better than the other? Both systems have many similarities. LRIT feeds into Project Camelot and it's based on ship reports, whereas AIS is automatically generated. AIS and LRIT were developed in stovepipes. The developers always knew AIS by satellite would be a check on LRIT. AIS from space is used as a ship tracking tool and collision avoidance. AIS was not intended as a security tool. Use of LRIT allows ships under attack to continue to transmit their location. AIS is too easy to intercept, whereas LRIT is security related and is much more difficult to intercept.
- Success in the U.K. evolved over 50 years. Success in Somalia is a product of that evolution. Relationships are getting better and stronger based on that evolution. We know who to go to, but it isn't technology, it's a phone call.

Breakout Sessions

Breakout Session Topic 1: Changing Frameworks
"Interconnecting Maritime Centers into a Global Grid. Getting the right information to those who need it, quickly."

Session Moderator
CAPT Russell Pegg, UK Royal Navy
www.royalnavy.mod.uk

51 The European Union's European Security and Defence Policy (ESDP) includes the gradual framing of a common defense policy which might in time lead to a common defense. The ESDP aims to allow the Union to develop its civilian and military capacities for crisis management and conflict prevention at international level, thus helping to maintain peace and international security, in accordance with the United Nations Charter. Source: European Union, http://europa.eu/scadplus/glossary/european_security_defence_policy_en.htm.

52 The MAOC-N was established in Lisbon in 2007 to combat drug smuggling in the European Union. For more information, please see The Maritime Analysis and Operations Center Perspective presented by Mr. Conor Shields in Breakout Session Topic 1: Changing Frameworks: Interconnecting Maritime Centers into a Global Grid.

Maritime Exchange Perspective

Mr. John E. Veentjer
Executive Director
Marine Exchange of Puget Sound
www.marineexhangesea.com

What data should we be sharing globally? Marine exchanges share information generally for the purpose of safety. Information subscription services gather information from multiple sources and monitor vessels 24/7. With Maritime Info Services of North America (MISNA), customers are private vessel operators and public agencies with maritime interests. MISNA owns 120 plus AIS receivers covering approximately 250,000 square miles of MDA. That includes electronic chart replay capability from AIS data stored for up to two years. Maritime Exchanges provide automated notifications along with monitoring of the "area to be avoided."

Singapore MDA Perspective

COL Chua Meng Seng
Deputy Commander, Maritime Security Task Force
Republic of Singapore Navy
www.mindef.gov.sg

The Maritime Security Task Force (MSFT), a SAF[53]-Level integrated taskforce, was established this year because of the continue threats. Terrorists are continually trying to find ways to infiltrate the increasingly complex Maritime Domain. We cannot use same approach as we have in the past. No single agency national or international can handle it alone. Through collaborative deterrence with EiS[54] and MSSP[55], incidents in the Malacca Strait dropped from 38 in 2004 to four in 2008.

Singapore National Initiatives are to establish bilateral linkages first; bilateral agreements have yielded better results than multilateral. Getting multiple players in a room together creates an environment in which the barriers come up. Establish new behaviors over time and scan outliers to discover emerging threats. Another tactic is the Maritime Info Sharing Exercises; these exercises allow partners to get used to sharing information and work out wrinkles in the system. It's important to think big but start small, and understand it's a long road.

Regional initiatives include socializing the value of information sharing. Collaboration in maritime security includes the Open and Analyzed Shipping Information System (OASIS) and the Sense-Making Analysis and Research Tool (SMART).

---

53 Singapore Armed Forces: the military arm of the Singapore Ministry of Defence.

54 "Eyes in the Sky" (EiS) combined maritime air patrols, initially conducted over the Straits of Malacca and Singapore by Singapore, Malaysia, Indonesia, and Thailand as part of the Malacca Straits Security Initiative (MSSI). EiS patrols respect the sovereignty and territorial integrity of the littoral states. Other nations are invited to participate. EiS is one element of The Malacca Strait Patrols (MSP) which also include MSSP and the Intelligence Exchange Group (IEG). Source: Singapore Ministry of Defence, www.mindef.gov.sg.

55 The Malacca Strait Sea Patrol (MSSP). Indonesia, Malaysia and Singapore launched the trilateral Malacca Strait Sea Patrol in July 2004. Under this arrangement, the participating states conduct co-ordinated patrols while facilitating the sharing of information between ships and the Monitoring and Action Agency (MAA). Source: Singapore Ministry of Defence, www.mindef.gov.sg.

This year we opened the Information Fusion Centre (IFC). It brings together human intervention with collective judgment, enabling technology, and integrated RSN[56]-ILO[57] team, and extensive linkages. We are letting 100 flowers bloom[58]. As more countries embrace information sharing, the closer we shall be.

Maritime Analysis and Operations Center Perspective

Mr. Conor Shields
Manager
Maritime Analysis and Operations Center Lisbon

The European Union Drugs Strategy program is improving coordination and cooperation at the national, European, and international levels. The threats are small vessels that are not transmitting AIS. The information flow for intelligence needs to be declassified and available in a central repository.

To date, we have prosecuted in nine different countries. Assets are used from 14 countries and personnel from 15 countries. Results include seizure of 43 tons of cocaine. Intelligence is shared among countries before moving to operational stage. How do we make this work? It's an equal partnership. Everyone has an equal say, even if they do not have any intelligence to contribute on a particular issue. Shift from "Pride of Ownership" to "Pride of Mission Accomplishment." Make sure everyone involved takes credit for the success.

Participant Discussion:

- What is the inter-linkage with INTERPOL / EUROPOL? Member states are to tell EUROPOL about all the investigations that they have going, but that is not happening. The MAOC has a reasonable relationship with INTERPOL. INTERPOL has offered access to their stolen vessel database. There are no noticeable barriers. INTERPOL has sent assets to help in a bust.
- Not only are there national, regional, etc. stovepipes, but now we see functional stovepipes just focusing on drug interdiction, piracy, etc. And not only do we have fusion centers but now there are interagency operations centers. The counter-drug community has ironed out many rough spots and produces actionable intelligence efficiently. The counter-terrorism community should take a step back and look to counter-drug as a model. We may be making counter-terrorism more complicated than it needs to be. We should tackle terrorism as a criminal activity.
- Australia is using a strategy of creating relationships with its closest neighbors before reaching a little further out. Australia is taking a baby-steps approach rather than tackling the world all at once.

56 Republic of Singapore Navy

57 International Liaison Officers

58 "Let a hundred flowers bloom, let a hundred schools of thought contend." Mao Zedong, suggesting the best system is created by encouraging the expression of competing concepts and constructive criticism.

Breakout Session Topic 2: Changing Perceptions
"Increasing Industry and Government Dialog Points. Increasing the level of understanding of each other's MS/MA issues and concerns."

Session Moderator
Mr. Lennis Fludd
Office of Security
U.S. Maritime Administration (MARAD)
U.S. Department of Transportation
Chief of Staff
Office of Global Maritime Situational Awareness (OGMSA)
www.gmsa.gov

Marine Offshore Industry Perspective

Mr. Ken Wells
President
Offshore Marine Service Association
www.offshoremarine.org

The Jones Act has not been well enforced with offshore industry because some definitions are unclear. In the process of tracking foreign vessels operating in the offshore industry, we've discovered there are a lot of data points, with many agencies collecting, but nobody coordinating. Only now are they starting to coordinate. When they do coordinate, they'll be overwhelmed by data. Software is important to track vessels, to ensure they are actually going where they say they are and will help us to understand the data.

We were tracking data on foreign vessels to enforce the law to protect our business. We learned what info is available on vessels. There's a lot of information available. If you could gather it all together you'd have a fairly complete picture. As we've looked at these vessels, they leave port and turn off their AIS. Why? What's the underlying reason? Vessels file with CBP saying they're on a voyage to nowhere – what are they hiding? These issues should concern security in addition to Jones Act enforcement.

U.S. Coast Guard AIS Data Sharing Policy

CAPT Curtis L. Dubay, USCG (Ret.), P.E.
Office of Maritime Domain Awareness and Information Sharing (CG-51-M)
Office of Department of Homeland Security MDA Executive Agent
U.S. Coast Guard
U.S. Department of Homeland Security
www.uscg.mil/hq/cg5/cg51.asp

We all interpret the same information differently based on our own framework. Combining safety equities, security, and environmental, people don't see the same information the same way. Once you have a mechanism to receive AIS data, what can you do with it to make things better? There are several ways to address safety, security, environment and economy better. Why share AIS? The IMO condemns irresponsible sharing of AIS. We support that view. But if done responsibly, it enhances safety, facilitates commerce, improves MDA, and improves life on the water.

How does the Coast Guard view domain awareness? Think geographic and temporal – approach zones, coast, ports, oceanic. We're approaching layers of MDA with LRIT, the Nationwide AIS collection system, Interagency Operations Centers, radars, cameras, etc. We are trying to develop a concept of how to share marine information, but decided to try something easier, first: sharing AIS. That turned out to have many challenges we're working through.

Ocean Policy Development & Marine Spatial Planning

Dr. John Oliver
Senior Ocean Policy & Programs Advisor
Office of Policy Integration (CG-53)
U.S. Coast Guard
U.S. Department of Homeland Security
www.uscg.mil/hq/cg5/cg53.asp

The Interagency Ocean Task Force was established in 12 June 2009; working committees include Policy, Governance, Implementation, Public Outreach and Maritime. The expectations and deadlines of the task force are:

- Phase 1: Completed, starting with a roll out of the report and a 45 day window will open for public report
- Phase 2: Marine Spatial Planning – UNESCO defines it as "a public process of analyzing and allocating the spatial and temporal distribution of human activities in marine areas to achieve ecological economic and social objectives that have been specified through the process."

Ecosystem-Based Management is defined as an integrated approach to management that considers the entire ecosystem including humans; goal is to maintain ecosystem in a healthy.

President Obama wanted effective framework for effective marine spatial planning, with it a public process that analyzes and allocates the spatial and temporal distribution of human activities in marine areas to achieve ecological, economic, and social objectives that have been specific through a political process. The Taskforce is to develop a framework that will provide the effective, comprehensive ecosystem-based management system for the long-term conservation and use of the ocean, coastal areas, and Great Lakes. One purpose of taskforce is obtaining stakeholder input and to date 24 meetings have been held with various stakeholders. Awareness is essential, which is why this GMISS project is essential. We need input on how this impacts industry.[59]

Maritime Information Sharing Taskforce (MIST)

Ms. Wendy Walsh
Homeland Defense & Security Coordinator
Naval Postgraduate School
U.S. Navy
www.chds.us

The challenge we see at the Maritime Information Sharing Taskforce (MIST) is how to include the private sector in MDA efforts, provide value to them, and gather local perspectives of practitioners. The purpose

59 For more information, website: www.whitehouse.gov/administration/eop/ceq/initiatives/oceans.

of MIST is to provide a process for 2-way sharing of information and provide a forum for mutual problem-solving around MDA issues. Current sponsors and stakeholders are Naval Postgraduate School, MARAD, USCG, OGMSA, GMAII, CBP, Immigration and Customs Enforcement, the Joint Terrorism Task Force, NCAGS, and GMISS.

To date, we have piloted at MIST Long Beach/Los Angeles in August 2008. In May 2009, we expanded for MIST Puget Sound; FY2010 MIST Honolulu HI (Nov 2009) and MIST NY/NJ in May 2010. Being responsive to the needs of our stakeholders is key to success. We are collaborating with the Coast Guard's Centers of Expertise and weaving their research into what we've found.

Breakout Session Topic 3: Changing Policies "Increasing Industry Involvement in Policy Making"

Session Moderator
Mr. Joseph J. Cox
President & CEO
Chamber of Shipping of America
www.knowships.org

U.S. Coast Guard Perspective

Mr. Dana Goward
Office of MDA and Information Sharing (CG-51-M)
Office of the Department of Homeland Security MDA Executive Agent
U.S. Coast Guard
U.S. Department of Homeland Security
www.uscg.mil/hq/cg5/cg51.asp

The piracy issue is about reforming policies, extensive outreach to industry, what kind of best practices, what kind of flexibility to should be built into policies. And there is a need to collaborate with industry. On the USCG website, there is a wide range of information dealing with anti-piracy.

Maritime Industry Perspective

Mr. James Christodoulou
CEO
Industrial Shipping Enterprise
www.industrialships.com

Piracy is not just a U.S. flagged problem; 95% of the tonnage is internationally flagged and this piracy issues requires an international response. After experiencing a hijacking first hand as a ship owner, there are three phases to understand: pre-board, hijack, and post-hijack. Pre-voyage planning is critical, the financial analysis of going through these areas, or going around, weather projections, threat assessment of the region – other agencies can help the ship owner with these projections, transit time, speed, convoy or not? Unless these measures are lethal, they will not deter an attack. At the end of the day, it's a human crisis; the safety of the crew on the ship is the most important issue.

What has been learned from the hijacking is that personal contact with the families of the crew is critical; knowing personal information about each crew members is the job of the ship owner. A ship hijacking is a human issue.

Having logistics in place before the hijack is critical, having codes set up between the crew and the ship owner so they can communicate effectively. Negotiations are difficult; the ship owner must be methodical because mistakes cannot be afforded. By identifying your objective and mission, you are able to focus on that and make sure every act and decision you make is in line with these items. A company needs to determine before the voyage if they are going to pay a ransom and put into place a plan to get cash to the area immediately.

The post-hijack phase is as critical as the first two phases; having a replacement crew in place is vital. Furthermore, it is important to offer services to the crew, including post traumatic stress disorder (PTSD) assistance. Again, a human issue, post crisis it is important to have communication with the crew to let them know what services are available to them and how they can be helped.

Armed Security Pitfalls

Mr. Charles Papavizas, Esq.
Partner
Winston & Strawn, LLP
www.winston.com

Maersk Alabama and Liberty Sun are the two incidents known by the U.S. public. Both were attacked this year, but the Liberty Sun was not boarded, only shot at. There are liabilities regarding carrying firearms on board a ship. If you are a merchant vessel you have the right to engage in self defense, though the legal ramifications if you do are not spelled out. This statue is from 1819 and last time it was interpreted was 1864.

The international maritime community is against putting firearms on commercial vessels. The International Traffic in Arms Regulations (ITAR) – written by the State Department – states virtually all defense articles including firearms are not allowed to leave the U.S. Progress has been made to ITAR as interpretations have shifted and it is clear some self defense weapons are allowed with licenses, but must be licenses regarding to the country.

The Cummings Amendment[60] requires Secretary of Defense to provide embarked military security teams to U.S. commercial vessels operating in high risk areas and determined to beat risk of being boarded. U.S. Navy is opposed because they say they do not have the resources to protect these ships. The ports that commercial vessels are most visiting do not allow firearms and to obtain a license is economically unfeasible.

Participant Discussion:

- Is it sufficient to just contain the situation (piracy)? Shouldn't we be eliminating the situation? We just proceed with the idea of eliminating the problem – however the problem is an entire nation-state and the Department of State has been unable to make progress.
- What does industry think the relationship between industry and the government should be? Why is it that this industry doesn't have that relationship?

60 For notes on the Cummings Amendment, please see An Industry Perspective on Piracy, presented by Mr. Phillip Shapiro during the second plenary session, Industry–Government Dialog: Digging Deeper.

Participant Discussion:

- Industry realizes the threat of piracy is low among the levels of threat against the United States. Industry wants firepower to be brought to bear upon the pirates, but *not* from commercial ships because of the risk of retaliation. Uniformed individuals have the luxury of being protected from retaliation whereas commercial crewmembers do not have that protection. The shipping industry is fragmented because of the small percentage of U.S. flagged shipped, which might have the protection of the U.S. Navy. Unless we try an international force to escort these ships through these dangerous areas, how will we know the success rate?

Symposium Working Groups

Working Group A
"Building a Global Maritime Information Exchange Grid, Is It Possible?"

Lead	**Co-lead**
CAPT Andy Bjork, USN	Capt Ralph Nieves, USN
U.S. Fleet Forces Command	Chief, Data Sharing & Infrastructure Branch
U.S. Navy	Office of Global Maritime Situational Awareness (OGMSA)
www.cffc.navy.mil/	www.gmsa.gov

New Zealand Perspective

Mr. Richard Davies
Manager, National Maritime Coordination Center
New Zealand Customs Service
www.customs.govt.nz

Need clarification of information necessary or required by the Maritime Industry as well as by intelligence and governmental sources. Without identifying the exact information both parties need there is less likely to be a clear exchange of information. What do we need and what for? Seek out information via standard search modes currently in use. That is to say, use of key words, etc. However, this presupposes that there is access to data bases owned by interested parties.

Limited resources are everybody's problem. Governments do have enough resources; they just don't have enough resources to do their missions poorly. If identified governments could contribute personnel or equipment to a "coalition" sort of clearinghouse those people could perform the required research, sharing, and coordinating.

Collect info from government agencies or public sources. Who is going to collect it and where is the repository for this information? Who will have access to it? Are we going to protect intelligence sources through a "clearance" process for different stakeholders? Each nation is able to show what they have done nationally but more importantly, what can they share internationally that can help others in the region? The access to these databases is going to have to be arranged. Most agencies are very proprietary about their information and who they will share it with. We have to get past this if we are to move forward in an effective manner. These points were well identified and discussed yesterday. When the discussion deals with the lack of trust, the question is what have you done to build relationships throughout a region or within a particular country, ministry, or agency?

Canadian Perspective

Mr. Tom Fredericks
Marine Security Operations Centre (East)
Royal Canadian Mounted Police (RCMP)
www.rcmp-grc.gc.ca

Given the small fraction of international participation at this conference, how can we have a symposium without inviting representatives from the many international port and maritime organizations around the world? Where are the IMO, APEC, PMAESA, SPC, OAS, EU, and others? These organizations need to be invited too: WCO, IOTC, SAARPSCO, MARLO.

Does industry perceive they are treated as a customer? Government does not develop programs specifically for industry. Increasing costs for industry without their input is irresponsible.

Single Web Portal access to U.S. Government Maritime Information

Mr. Robert L. Hall, Jr.
Senior Enterprise Architect
U.S. Office of the Director of National Intelligence (ODNI)
www.dni.gov

What's the definition of information? What are we putting on the web? What are the useful feeds of information that government wants from industry? What does industry want from government?

There will have to be an incentive to either choose one portal, because we all know there will be many folks that have their heart and soul into their own project portals for capturing maritime domain information that will no longer have a place to hang their hat. We will need to manage this threat, to further future collaboration. A simple commitment to maintain watch and answer queries will go a long way and be a major achievement from this conference to kick off global info sharing.

Given that English is the international language, there maybe a need to also provide translations into French and Spanish. English is used and is standard in the aviation community.

The civilian approach sounds more user friendly, but we must remember our necessity to protect critical information. Therefore, if we insist on sharing databases, we will come up against a wall and not make any progress. It appears we are attempting to build a network without first doing the global engagements, meeting before the meeting, to determine who are the customers, what are the common elements of information everyone is willing to share, how the information will be used, how the information will be stored and safeguarded, and how will it be funded. If there is a commercial need then there is a commercial benefit, then the funding could be another cost of doing business, which certainly beats paying a ransom or the time and resources to provide maritime emergency assistance. Why not include industry at this point so both sides can formulate policy as well as account for the others requirements. Keeping their hand on our pulse is insufficient. It has to be a meaningful exchange and inclusion in the process.

Working Group Discussion Highlights:

Discussion Question: What are the advantages/disadvantages of linking together regional Maritime Operation Centers, Fusion Centers, Maritime Exchanges, Government Maritime Information Hubs into a single grid?

GMISS website should include a map that allows the user to click on and identify operations centers around the world. Link should include contact info and area of responsibility for the Ops Centers. Slide by Capt Bjork (USCG) showing NCAGS around the world was first clear acknowledgement that GMISS conference is meant to be global rather than parochial. Naval Co-operation and Guidance for Shipping (NCAGS) is a naval organization with members who are trained to establish and provide advice for safe passage of merchant ships worldwide, during times of peace, tension, crisis and war. NCAGS personnel act as a liaison between military commanders and the civil authorities.

Individual national, regional, functional operational centers should look at developing a non classified web portal that they are willing to make available to any and all customers. If industry and others have knowledge of where to go to get the information that is of value to them in, for example passage planning, is that not in essence a global maritime info system?

Discussion Question: Is the barrier to information sharing a technology issue, a policy or cultural issue?

Private industry is no different than law enforcement or government. The airline industry shares data multi-laterally, why not the maritime industry? It is primarily a policy issue. Twisting wires between systems is relatively easy; establishment of policy basis alleviates some of the cultural issues but not all.

Ideas included:

- What about starting with basic information sharing (e.g. AIS data).
- Non-classified, lowest level for a global grid... build the trust and relationship with existing technology.
- We should work towards identifying one or two "actionable" items for Industry and one or two for Government with regard to the end results of this grid.
- Define what an "information sharing agreement" is (the elements it consists of) and when it is useful to have them documented.
- Develop a coherent framework for determining who needs to share what information, when (which preceding event), and with whom.
- Define the essential elements of information that need to be sent/received in different contexts (scenarios, roles, tasks).
- Create best-practice models for how information needs to flow in high-risk scenarios, and then have each jurisdiction adapt them as needed.
- Social networking impacts forms and types of agreements. Are we digital dinosaurs or neophytes? Some culturals (dinners, teas, special dates) still require relationship building as part of building the necessary trust towards building agreements. It takes time and acumen about the necessary players.

Working Group Discussion Highlights:

Suggested that key administrators spend time at Joint Interagency Task Force South (JIATF South) is a multiservice, multiagency joint task force of the United States armed forces based at Naval Air Station Key West (Truman Annex), Key West, Florida. It conducts counter illicit trafficking operations, intelligence fusion and multi-sensor correlation to detect, monitor, and handoff suspected illicit trafficking targets; promotes security cooperation and coordinates country team and partner nation initiatives in order to defeat the flow of illicit traffic. It is associated with the United States Southern Command but is under Coast Guard leadership.

Working Group B
"Bridging the Understanding Gap between Maritime Industry and Government"

Lead	**Co-Lead**
Mr. Andy Grasso	CDR James Feldkamp, USN
Sea Operations Manager	Office of Global Maritime Situational Awareness (OGMSA)
American Roll-on, Roll Off Carriers	www.gmsa.gov
www.arrcnet.com	

Interagency Investment Strategy Report

Mr. Joseph Milligan
Chair, Interagency Solutions Analysis Working Group,
Director, Capabilities-Based Planning (CBP)
Office of the Department of Defense Executive Agent for MDA
U.S. Department of Defense
www.dodeaformda.navy.mil

Interagency Solutions Analysis (IASA) MDA capability areas are management, collection, fusion, analysis, and dissemination. IASA is developing a series of workshops – first workshop in December – looking for participation from industry and academia. Government needs to understand the industry it is regulating.

U.S. Coast Guard Centers of Knowledge

CAPT Gordon Loebl, USCG
Chief, Office of Quality Assurance and Traveling Inspectors
U.S. Coast Guard
U.S. Department of Homeland Security
www.uscg.mil/hq/cg5/cg546.asp

USCG Marine Safety Performance Plan FY 2009-2014 is in response to criticism that USCG had shifted focus away from Safety. USCG Miami set themselves up as a "Center of Excellence" for cruise ship industry since it handles 90% of all cruise ships. Place where personnel may take classes and take advantage of expertise in that region. National Centers of Excellence Capabilities: repository of technical competence & expertise, venues for professional development & exchange with industry, improve competence/promote consistency, consultation, professional training exchanges, ensure uniform application of regulations/policy/doctrine/TTP, developing curriculum for exportable & resident training.

Maritime Training Perspective

Mr. John Tomoney
Global Maritime & Transportation School (GMATS)
U.S. Merchant Marine Academy (USMMA), King's Point, NY
www.gmats.usmma.edu

The U.S. Merchant Marine Academy has cutting edge training available in the following areas:

- Training for port security personnel
- Anti-piracy training
- Vessel Vulnerability Assessment Training
- Strategic Overview to End to End Supply Chain Security
- Created a program for the Swiss Navy and Maritime Industry

Working Group Discussion Highlights:

Discussion Question: How do we facilitate deeper industry involvement in the maritime policy formulation process?

Need direction to get buy-in from private industry and the following are suggestions on how to do this:

- Advisory panel comprised of industry leaders to advise the MDA Stakeholders Board.
- Area Maritime Security Committees – have role in policy issues at local level.
- How do we standardize across area maritime security committees?
- At National level – CBP is not present in creating policy in Maritime Security. CPB will resist forming communications relationships that are already being handled within the maritime domain. An issue of duplication of effort ad infinitum.
- We are regulated by a government entity that doesn't understand our industry. What is the mood of the U.S. Merchant Marines to the regulatory environment, the international regulatory environment?
- Does the government/industry relationship begin in the classroom?
- Boarding opportunity to petty and officers for industry training – this should be a requirement, not voluntary, and shouldn't hurt promotion.
    - What's in it for me as an industry person? It's an excellent idea, but it becomes an administrative nightmare for the company with the overhead involved.
    - Working with Maritime Unions – Represent population friendly to our interests & they have training facilities that train all of their members.
- There also needs to be a baseline for training, discussed that the MDA Stakeholders Board needs to be involved in this.

Working Group Discussion Highlights:

The issue was also discussed that mariners are no longer treated by the industry/citizens as professionals, they are no longer getting the respect they deserve by the industry, government and culture. We cannot ask the crew members to buy in on these issues if you are not treating them with respect. For each ship there are 2 senior level officers (2 Masters, 2 CEs, 2 Chiefs, etc.) Two full crews have to be trained on such regulations as indigenous species in ballast water in various regions. Crews are opting not to sail to U.S. Ports because of the restrictions that are placed on ships.

Working Group C
"Resolving Information Privacy, Proprietary & Classification Concerns"

Lead	**Co-Lead**
CAPT David Sanders, JAGC, USN,	Ms. Wendy Walsh
Legal Counsel	Homeland Defense & Security Coordinator
Office of Global Maritime Situational Awareness (OGMSA)	Naval Postgraduate School
www.gmsa.gov	U.S. Navy
	www.chds.us

U.S. Government Information Sharing Barrier Resolution Process

Captain David Sanders, JAGC, USN
Legal Counsel
Office of Global Maritime Situational Awareness (OGMSA)
www.gmsa.gov

Information sharing is based on trust. Policy must make sense and reflect a two way street between private sector and government. Private companies are concerned about cost, they answer to their shareholders. Any additional resources or requirements on industry cost money. Industry loses trust in government when it is not responsive; unresponsive because of cumbersome intra-government info sharing. It's difficult to respond to something you don't know about.

Classified and unclassified information sharing is a huge problem barrier. What's also a problem is our inability to share unclassified information well. Another barrier is that government needs to be open to receive information, and information needs to be pushed out to international and private sector partners. If people (constituents) believe their government is not responsive, they begin to lose trust in their government. Industry must challenge their government and hold them accountable.

Maritime Industry Perspective

Captain Paul Londynsky
Vice President of Safety, Quality & Environmental Affairs and Chief Security Officer
Matson Navigation Company, Inc.
www.matson.com

The primary problem is trust. In the Seattle stowaway incident MV Rotterdam, 1996, the carrier would be in trouble regardless of time or agent of discovery...reporting is disincentivized. One nation's

stowaway is another nation's terrorist - where should accountability start if not with the carrier? Is the whistleblower program transferrable to the maritime realm for non-attribution reporting?

Global AIS Coverage: an Industry/Government Co-op opportunity?

Mr. Moses Calouro
President
Maritime Information Systems, Inc.
www.misdevelopment.com

SOLAS requires AIS transmitting for large vessels. AIS requirement planned to be extended to "everything that floats" which could present a saturation problem in heavily populated Asian ports. AIS Pros: Real-time, advanced notice of traffic ahead, saves man power or time. AIS Cons: Can be turned off, fields can be changed to misidentify vessels characteristics. Unwarranted government surveillance issues – privacy vs. security. Connect all the dots for more complete MDA. A plethora of information is available, let's put it all together so everyone is more effective.

Working Group Discussion Highlights:

Discussion Question: What can be done to reduce the perceived lack of trust and reciprocity from government to industry with regards to information access/sharing? Is it even an issue?

Establish a whistle-blower Law to encourage self reporting of suspicious activity, stowaways, trespassing, and criminal activity. Private industry would be more likely to self report if there is no reciprocity, fines, legal costs. The return on investment is measureable.

Discussion Question: Does industry have an information sharing barrier/dispute resolution process to accommodate concerns of the sharing of proprietary information to the betterment of industry efficiency?

Encourage greater use of data that is currently available, and consider regional proliferation and global consolidation of AIS data.

Discussion Question: How/when is the government going to stop over-classification? Is it crucial to the overall Maritime Information sharing effort?

A policy to mandate information sharing is needed, as well as a dispute resolution procedure. Furthermore, develop information sharing awareness training to improve intra-government information sharing, similar to information assurance or sexual harassment training currently required for government personnel.

Working Group D
"Piracy: A Model of Co-developed, Mutually Beneficial Policies?"

Lead	**Co-Lead**
Mr. Giles Noakes	CAPT Dale Ferrier, USCG
Chief Maritime Security Officer	Chief, Plans & Policy Branch
Baltic and International Marine Council (BIMCO)	Office of Global Maritime Situational Awareness (OGMSA)
www.bimco.org	www.gmsa.gov

Note: *The piracy working group was added to the program in coordination with the Marine Log organization, which merged its 2009 Combating Piracy Conference into GMISS because the issues likely to be addressed were reflected in the overall aims of improving information sharing and intelligence sharing. The precipitous rise in piracy during 2009, particularly in the Gulf of Aden, prompted an unprecedented surge in international maritime cooperation, including an integral increase in maritime information sharing, among a broad range of powers, including the United States, Russia, the European Union, China, Australia, India, Pakistan, Canada, Singapore and Turkey, to coordinate anti-piracy actions. Therefore, the GMISS piracy working group was asked to address whether the international response to piracy should serve as a model of co-developed, mutually beneficial policies.*

BIMCO Perspective

Mr. Giles Noakes
Chief Maritime Security Officer
Baltic and International Marine Council (BIMCO)
www.bimco.org

Nations only have a "single pool of forces" and expecting more than 40 ships in the Gulf of Aden region is unrealistic. Currently the benefit to pirates is greater than the risk. Industry cannot rely on (individual) support from navies. Industry has a responsibility that will require spending own resources (e.g. wait for escort if so required). The Web-based Automated Vessel Risk Assessment tool, developed in cooperation with the IMO and security consultants, is an example of an information sharing tool that can help decision makers. It is important to consider alternative approaches to the resolution of the problem. A significant issue is that there is no single point of contact for a global industry to go to.

Industry has developed best management practices and must be able to rely on governments and navies to ensure the rule of law is enforced in this international space, a longstanding role of navies. How much is industry willing to pay additional for this service that doesn't finance itself?

USCG Security Directives & IMO Guidelines

Mr. Charles “Bud” Darr
Office of Maritime & International Law
U.S. Coast Guard
U.S. Department of Homeland Security
http://www.uscg.mil/legal/

There are subtle differences between MARSEC Directive 104-6[61] and industry best management practices (BMP). Information within this MARSEC Directive is designated Sensitive Security Information (SSI) and is not subject to public release. Compliance with industry BMP will not make a U.S. vessel compliant with 104-6. More information is available on the Coast Guard Website.

Task Force 151[62] currently consists of three ships, the USS San Antonio, the USS Mahan, and the HMS Portland. It is engaged in protecting a corridor in the Gulf of Aden that civilian vessels are strongly urged

61 Maritime Security Directive 104-6; Guidance for U.S. Vessels operating in High Risk Waters (Revision 2) was published by the U.S. Coast Guard in May 2009.

62 Task Force 151 is a counter-piracy naval coalition established specifically to address the threat of Somali piracy.

to use as an effort to limit access by the pirates to shipping. The area of responsibility is about 1.1 million square miles of sea.

U.S. Maritime Administration Perspective

Mr. Owen Doherty
Director, Office of Security
U.S. Maritime Administration (MARAD)
U.S. Department of Transportation
www.marad.dot.gov

It is my understanding of the industry perspective is that Task Forces 150[63] and 151 are rather narrowly focused and not terribly cohesive regarding mission statement, rules of engagement and scope, and therefore are limited in their ability to fight overall piracy in the region. TF 150 and 151 do have different missions. TF 150's mission is strictly anti-terrorism. Therefore, TF 150 is not to conduct anti-piracy tasks other than under very particular circumstances. UNCLOS[64] does not help since military forces need dedicated missions/mandates to act and cannot act upon international law by creating their own mission as the situation might dictate.

It may be short sighted and naive to not consider the capacity for terrorism that the pirates present and therefore not take decisive action prior to that development, considering the threat to the unmolested flow of international trade, particularly the petroleum trade. It is dangerous to allow the distinction between piracy and terrorism, and the burden counter-piracy places on military resources dedicated to the War on Terror, to prevent effective action before this capacity is exploited by terrorists.

A voluntary, rather than regulatory, approach has been enormously successful. We should learn from the International Ship and Port Facility Security experience that regulation is often too slow and often does not end up addressing evolving maritime threats. The ISPS Code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Having come into force in 2004, it prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to "detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade."

The Ship Operations Cooperative Program, in cooperation with U.S. government and industry partners, is working on training guidance and a course syllabus, as well as a training video. SOCP addresses and promotes commercial operations through the identification, development, and application of new methods, procedures, and technologies. SOCP's overall objective is to improve the competitiveness, productivity, efficiency, safety, and environmental responsiveness of U.S. vessel operations. All U.S. based vessel operators and organizations that support vessel operations are eligible to participate in the program. With the support of the Maritime Administration, industry, labor, and government are working together to address common challenges and identify new solutions for improvements in ship operations. More information is available on MarView. Should MARAD take the lead in assessing the value of technology solution sets and giving a certification such as DHS does for anti-terrorism technology?

63 Task Force 150 is a naval coalition established to to monitor, inspect, board, and stop suspect shipping to pursue the War of Terrorism and support Operation Enduring Freedom in the Horn of Africa region.

64 United Nations Convention on the Law of the Sea, opened for signature Dec. 10, 1982 and entered into force Nov. 16, 1994, defines the rights and responsibilities of nations in their use of the world's oceans. The United States is one of approximately 21 nations that have signed the convention but have not ratified it, although, the United States helped develop the convention and abides by the majority of its provisions.

Working Group Discussion Highlights:

Discussion Question: How well has the international maritime community responded to Piracy?

Response success can be measured by the success of mariners in fending off pirate attacks. The percentage of successful pirate attacks has decreased from 2008 to 2009. Response has been slow, inappropriate, and lacks alignment of national and international objectives. No clear international objectives and nation states have set their own objectives.

There is an international objective to combat piracy. The problem is in the execution. Nations have differing financial resources and differing security policy priorities. There should be a single point of contact with specific rules/information for transiting specific areas. There is no recognized, readily available phone number to dial with informed people on the other end standing by. Individual governments have policies that differ from the UN standards. Each nation has its own Rules of Engagement with regard to piracy.

- Action Item: There should be a single point of contact. This should be a coordination center. Possibly one of the new Rescue Centers. Possibly MSC-HOA? This center should be in a place where ship owners want to do business (not in Djibouti).

Discussion Question: Do the policies fit the issues?

What is the issue we are trying to develop policies to solve? There is a subtle yet profound difference between ensuring safe passage of vessels and stopping piracy in Somali region. Furthermore, the definition of piracy is not clear: armed fisherman or pirate? What internationally recognized definition can be used to give navies the right to seize, and courts to convict, a pirate?

There is a need for a single point of contact for information and reporting. MSC HoA and UKMTO are working very closely together and can be seen as the single point of contact. Inconsistent application of policies has hampered effective suppression of piracy.

Discussion Question: Can the Piracy response model be utilized to respond to other maritime crisis?

If the model includes endless debate over jurisdiction, liability, military territorial rights etc., accompanied by incremental policies from multiple bodies devoid of universal consensus, then probably not. Maritime Operational Threat Response Plan aims for coordinated United States Government response to threats against the United States and its interests in the maritime domain by establishing roles and responsibilities that enable the government to respond quickly and decisively.

Coordination and response to oil/hazmat discharges seems to have been a more effective model for international response and cooperation. The model of multi-national response when driven by international concerns (tsunami, disaster relief) shows how a cooperative effort can work. Relief aid does not have Rules of Engagement issues, so it requires a more dedicated approach. A cooperative effort requires a single point of contact. Publication 117 provides contact information aboard vessels to prevent hazards to shipping. This existing route should be tried to see if it works or if it needs to be fixed. Oil/Hazmat provides a clear distinction that you have to call the National Response Center. This model could be used for piracy reporting.

Discussion Question: What if piracy occurs elsewhere, do we have to re-invent the response?

Much of the work to combat piracy recently has been area-specific. Issue is that of robbery/crime against ships in nation state waters and how that can be combated in those states, especially where there is no strong central government to take action. What are other potential trouble spots? Could work with other troubled nations to head off the threat that they will become areas of piracy?

Working Group Discussion Highlights:

How can the international community best put pressure on nation states, such as Nigeria, to mitigate or eliminate the threat, especially while events are focused within territorial waters? Government to government engagement is essential. Who will prosecute pirates in the early stages (before the attack)? Will it be the failing nation states or will they invite other nations to come in and police their territory? Will response and success be mainly defined by the commitment and capability of the states off whose waters the events are occurring? Lessons being learned today should be incorporated into training for mariners – e.g. Vessel Security Officer Courses.

Working Group Presentations

Working Group A
"Building a Global Maritime Information Exchange Grid: Is It Possible"

Points of Discovery

- Need effective "industry/NGOs/multi-lateral governmental organizations/LEA" representation at information sharing discussions
- Individual national, regional and functional operational centers should look at developing/utilizing existing non classified web portals that they are willing to make available to any and all customers
- Need a meta-site listing maritime information sharing exchanges (government, NGO & industry) with a feedback loop for comments (and initiatives)
- An effective marketing strategy is required for improving information sharing between government/NGO/industry (i.e. The value/benefit of information sharing)
- Need governance of the global grid: Formal agreements, Memo of Understanding, Gentlemen's Agreement, some or all of the above?
- Panel needed for Essential Elements of Information (EEI) development
- How does an element fit into the maritime information sharing puzzle; Rings of Access / Attribute base Access Controls

Actionable Items

- Define the "as is" state (i.e. information sharing sites, exercises, collaborations/laws & polices, best practices) useable discoverable, accessible
- Develop meta site of maritime information exchanges
- Develop and implement a marketing plan for government/industry/NGO maritime information sharing
- Create a panel to define EEI

Ongoing Discussion Points and Recommendations

1) *Who can use it, how broad?* This will fall under the governance section of our actionable items to be further developed.

2) *Has the working group identified the information requirements*? Need to break that out, and identify what can be accomplished quickly, and then identify a broader view.

3) Are there existing meta sites? Are we going to review information out there to make sure there is not duplication of information/efforts?

4) Comment that the log-on information needs to be simplistic and a one time log-on.

5) How many people would like to assist with this working group? Approximately 20 people raised their hands.

Working Group B
"Bridging the Understanding Gap between Maritime Industry & Government"

Points of Discovery

- The government's lack of understanding of the private sector is one of the key challenges in the maritime industry. (For example, this industry is overwhelmed with regulations and there is a consensus within industry that the people writing the regulations do not have a clear understanding of the industry they are regulating.)
- Training is key to bridging the understanding gap between maritime industry and government. This training is a two-way street; government also needs to train industry on the regulatory process so that all stakeholders understand.

Actionable Items

- Research the environment and evaluate training and internships currently available within the maritime industry and determine what is still needed. It's important that this training be unclassified and examines existing inter-agency, inter-government, inter-industry training to establish a baseline for future programs. The deadline to begin this task is 31 December 2009 and the conclusions and recommendations will be presented at the next GMISS.
- Another issue that needs to be address is policy issues surrounding MDA. This working group requests that industry participate in the Maritime Domain Awareness Stakeholder Board that meets monthly, and requests this action take place by 31 December 2009. It is also requested that industry participate (by invitation) in Maritime Security Inter-Agency Policy Committee which reports to the National Security Council.

Ongoing Discussion Points and Recommendations

- We recommend for next GMISS this working group explore intermodal operations and regulatory issues surrounding MDA, e.g is there a national strategy? Also a review of the regulations to determine if there's overlap and/or archaic regulations. We also suggested that MTSNAC/CMTS be invited to GMISS.
- *MDA Stakeholders Board input valuable.* For example, the agencies we most interact with, such as USCG and CBP – for example CBP is not here today and they need to be involved in these discussions.
- *How many are interested in participating in this working group?* Approximately 10 people raised their hands.

Working Group C
"Resolving Information Privacy, Proprietary and Classification Concerns"

Points of Discovery

- The "trusted agent" in the area of information is needed to effectively disseminate maritime information; who is a trusted agent? Trusted agents need to push the classified information down to the right people in a non-classified form so that it is usable. Furthermore, these trusted agents need to receive information from people outside the government.

Actionable Items

- Develop pilot program (JIMDA & MIST) utilizing existing infrastructure to disseminate information.
- Expand America's Waterway Watch program to encompass all users. For example, where does a commercial ship call? When the call is received, is the operator trained to deal with the information?
- Consolidate regional proliferation and global consolidation of AIS data
- Examine use of a non-government organization to manage international governance options for Global AIS
- Uniform U.S. Government policy mandating interagency information sharing
- Develop information sharing dispute resolution procedure
- Develop training for information sharing professionals; transform the culture of "need to know" to "need to share"

Ongoing Discussion Points and Recommendations

- Maritime Information Reporting:
  - Government needs to limit impact of information reporting on industry operations. Often, government does not even use the information that costs the industry money to compile and report.
  - Industry needs protection from retribution for credible reporting to government.

Working Group D
"Piracy: A Model of Co-Developed, Mutually Beneficial Policies?"

Points of Discovery

- There are seemingly no clear objectives defined for or by the international community. Objectives in the main are only implicit and those that are explicit revolve around humanitarian aid protection.
- There is a clear requirement for a single point of contact for all information flow – reporting by industry and the dissemination of information to industry. The lead example of the UKMTO[65]/MSCHOA[66] was cited.

---

65 The United Kingdom Maritime Trade Operations office in Dubai acts as the primary point of contact for merchant vessels and liaison with military forces in the region.

66 The Maritime Security Centre – Horn of Africa, set up by the European Union as part of a European Security and Defence Policy initiative to combat piracy in the Horn of Africa, is a coordination center dedicated to safeguarding legitimate freedom of navigation in the light of increasing risks of pirate attack against merchant shipping in the region, in support of the UN Security Council's Resolutions (UNSCR) 1814, 1816 and 1838.

- There is a requirement for greater understanding by and between governments of industry commercial fundamentals across the spectrum of maritime trade; from charter party agreement legal implications through to the variety of maritime insurance issues.
- Ship owners have a duty of care to seafarers that national laws do not necessarily respect. The industry however is a global industry and the primary legislator is the IMO.
- Current inaction displays a lack of resolution on the part of many nation states and questions the credibility of overt military action.
- The current model has far too many constraints and complexities – politically, economically and tactically.
- Any maritime crises will require a point of contact and that this should be a single point for all issues of communications, command, control and information. This is essential to manage operations effectively. The use of UKMTO as the single focal point for operations, in this case, provides the lesson to learn.
- The co-ordination of industry and the military is a paradigm for future use to create an environment for safe shipping. The SHADE[67] co-operation is a classic example of such cooperation and co-ordination.
- Defensive measures espoused for the Gulf of Aden will in general apply to dealing with piracy anywhere in the world.
- Having developed and enhanced co-ordination and procedures between industry and the military, the confidence and communication that have been built up should not be lost.

Actionable Items

- There should be a clear agreed objective by the international community to repress and defeat piracy.
- Establish a single point of contact for all information flow, including reporting by industry and the dissemination of information to industry.
- Identify and develop the best course of action to educate government personnel that impact the maritime industry on industry commercial fundamentals.
- Better focus the debate within bodies such as the IMO on the ISPS codes and the duty of care to seafarers.
- Encourage those nation states that have not implemented maritime laws compelling arrest and prosecution of pirates under UNCLOS and SUA to do so as a matter of some urgency in order to provide a vital additional deterrent against piracy and pirates. Furthermore states should then be encouraged to implement those laws in a timely manner notwithstanding fears of future asylum seekers, etc.
- The right to "visit" under article 110 of UNCLOS[68] should be encouraged, particularly as a deterrent to the use of mother ships. In support of this action, encourage the use of sea riders, better defined

67 The Shared Awareness and Deconfliction (SHADE) group conducts monthly meetings in Bahrain to share information and ensure the effective coordination of military resources and counter-piracy efforts off the coast of Somalia. More than 30 nations have participated, as well as industry associations such as The International Association of Independent Tanker Owners.

as law enforcement officers from either the flag state of the warship concerned or those nations who have offered legal support.

- Develop a single point of contact for maritime crises.
- Build on the response models created by UKMTO and the SHADE group.
- Encourage industry to lobby the IMO to implement, through the ISPS codes and beyond the issue of guidelines contained in MSC[69] circulars[70], the generic content of such standards as the BMP and the industry "Blue Book."
- Ensure best practices and successes in repelling pirates are shared in a common environment to drive the inclusion of ship defensive measure in future ship design.
- Regularly record and review lessons learned to maintain coordination between industry and government developed thus far and preserve confidence in communication.
- Interested states and parties should continue to address capacity building in coastal states where similar underlying causes exist or could develop easily, in order to reduce the same potential risks.

Closing Remarks

Symposium Summary

Mr. Gary Seffel
Acting Director
Office of Global Maritime Situational Awareness (OGMSA)
www.gmsa.gov

OGMSA has gone over thousands of details for the past 12 months setting up this conference. No matter what we do, it does not work if you don't participate, so thank you very much.

The question was asked – Who's in charge? MDA is not just a U.S. federal effort, so not one entity can be in charge. For U.S. federal piece of the issue, the National Security Council coordinates for the President. It's also the responsibility of each state and local government and each has a set of sovereign powers. All entities need to stay engaged with each other, including the private sector, in order to make MDA a coherent issue.

68 UNCLOS Article 110. Right of visit. 1. Except where acts of interference derive from powers conferred by treaty, a warship which encounters on the high seas a foreign ship, other than a ship entitled to complete immunity in accordance with articles 95 and 96, is not justified in boarding it unless there is reasonable ground for suspecting that: (a) the ship is engaged in piracy; (b) the ship is engaged in the slave trade; (c) the ship is engaged in unauthorized broadcasting and the flag State of the warship has jurisdiction under article 109; (d) the ship is without nationality; or (e) though flying a foreign flag or refusing to show its flag, the ship is, in reality, of the same nationality as the warship. 2. In the cases provided for in paragraph 1, the warship may proceed to verify the ship's right to fly its flag. To this end, it may send a boat under the command of an officer to the suspected ship. If suspicion remains after the documents have been checked, it may proceed to a further examination on board the ship, which must be carried out with all possible consideration. 3. If the suspicions prove to be unfounded, and provided that the ship boarded has not committed any act justifying them, it shall be compensated for any loss or damage that may have been sustained. 4. These provisions apply mutatis mutandis to military aircraft. 5. These provisions also apply to any other duly authorized ships or aircraft clearly marked and identifiable as being on government service.

69 The Maritime Safety Committee of the IMO.

70 The IMO releases circulars to provide notifications and guidance to the maritime community. The Maritime Safety Committee has released a number of circulars relating to piracy, particularly near the Horn of Africa, including guidance and best practices for industry, and recommendations to governments for the suppression of piracy and armed robbery against ships.

There are strong opinions on every issue, such as piracy. Only by collaborating and building unity of effort can we make sure our solutions meet everyone's interests. This whole business is just an enabler. It's not a mission in itself, except for a few of us, it's a part time job enabling us to get our jobs done with safety, security, protecting the environment, fostering the economy.

Only by collaborating on this can we make sure it meets everyone's interests. We are making progress – it's not fast, we're gaining momentum, one-to-one relationships matter – the people you met here can help you do your job better. The technology and systems are there but polices get in the way. Three pronged approach to maritime relationship exchange – relationships, policy, and technology. We've set the priorities for going forward.

We need your continued help with the working groups. To get involved please visit www.gmsa.gov. We plan to release the final report from GMISS 2009 as soon as possible. Look for it on our website (www.gmsa.gov).

Appendix E
Recurring Themes during GMISS Sessions

ISSUE	OCCURENCES
Coordination	24
Need single govt. point of contact for industry to report suspicious behavior	Addressed to USCG Vice Commandant
Local LE needs single fed POC	Addressed to USCG Vice Commandant
Who's in charge of MDA?	Addressed to USCG Vice Commandant
Is NMIC in charge of MDA?	Addressed to NMIC Deputy Director
Who's in charge of MDA?	Addressed to N3 Joint Ops Director, USFF
Why doesn't Navy take charge of MDA?	Addressed to N3 Joint Ops Director, USFF
Biggest obstacle to industry info sharing is the lack of a single reporting 911 system	Dir of Govt Relations, American Shipping & Logistics Group
Who takes the lead on information sharing? Federal or state agencies?	Panel Discussion 1
Need better coordination between govt and private security providers	COPS Deputy Director
MD State DOT relationship w/ USCG and private sector was one of its greatest strengths on 9/11	Deputy Secretary of Transportation
Foreign navies need to know how to coord w/ U.S. Navy on MDA	Addressed to N3 Joint Ops Director, USFF
OSAC is looking for feedback from private and public sector to improve our system of information sharing	Acting Director, OSAC
Getting the private and public sectors in a room to work things out together is a lot of progress.	Senior Advisor – Intelligence, DHS
We have to clarify the requirements, which requires a lot of dialog	Senior Advisor – Intelligence, DHS
ODNI is trying to share threat information with people on the waterfront, but is looking for a focal point.	Panel Discussion 1
Info to industry: there's a state government with authority, so federal authority is in question.	Panel Discussion 1
These issues have been percolating without resolution for some time now, which is the source of frustration in this room.	Panel Discussion 1
In the U.S., it's not the absence of rules -- it's the proliferation of them that seems to lead to confusion.	Civil Liberties Protection Officer, ODNI
In tracking foreign vessels offshore, there are a lot of data points, with many agencies collecting, but nobody coordinating. Only now are they starting to coordinate. When they do coordinate, they'll be overwhelmed by data.	President, Offshore Marine Service Association
Started info sharing with something "simple" with AIS, but that has turned out to be difficult.	Office of CG-51
President Obama established a taskforce for an effective framework for effective marine spatial planning with a public process to analyze and allocate spatial and temporal distribution of human activities in marine areas to achieve ecological, economic, and social objectives that have been specific through a political process.	Senior Ocean Policy & Programs Advisor CG-53
Challenge we find is how to include the private sector in MDA efforts, provide value to them, and gather local perspectives of practitioners.	Homeland Defense & Security Coordinator, NPS
Without identifying the exact information both parties need there is less likely to be a clear exchange of information	Manager, NZ National Maritime Coordination Center
Why not include industry at this point in designing the architecture so both sides can formulate policy as well as account for the others requirements	Senior Enterprise Architect, ODNI
Industry Information Flow	16
Industry input to govt is critical to national security	Deputy Secretary of Transportation
Companies want to share, how do we get info to the Intel community?	Addressed to NMIC Deputy Director
Navy needs industry info for MDA	N3 Joint Ops Director, USFF
Need info sharing w/ industry to prosecute pirates	Assistant Sec for Political Military Affairs, Dept of State
Industry may not need specific intel, just what I need to do to protect assets	Panel Discussion 1
How does the information get from this incredible bureaucracy to the guy who needs to make a decision this morning?	Panel Discussion 1
It isn't technology. It's about getting the information from the people who have it to those who will use it immediately.	Panel Discussion 1
Government realizes that's the goal.	Panel Discussion 1
Intelligence is not essential – guidance on evolving precautions can be sufficient.	Panel Discussion 1

ISSUE	OCCURENCES
The maritime industry needs to expand and improve the current awareness systems.	Senior Director Innovation, Maersk Line
Maritime awareness tools on commercial vessels should not be viewed as intelligence systems. They are safety systems	Senior Director Innovation, Maersk Line
OMS Association is tracking data on foreign vessels to enforce the law to protect our business. There's a lot of information available. Gather it all together and you'd have a fairly complete picture.	President, Offshore Marine Service Association
Need clarification of information necessary or required by the Maritime Industry as well as by intelligence and governmental sources	Manager, NZ National Maritime Coordination Center
Government does not develop programs specifically for industry; Does industry perceive they are treated as a customer?	Marine Security Operations Centre (East), RCMP
What are the useful feeds of information that government wants from industry? What does industry want from government?	Senior Enterprise Architect, ODNI
Mutual Understanding	8
Govt needs better understanding of Industry	Addressed to USCG Vice Commandant
Govt/Industry need better understanding of each other	NMIC Director
Policy is being made that effects the functioning of the global supply chain system without appreciation for what those effects will actually be.	Senior VP, Maersk Line LTD
Implementing the CIKR ISE requires finding out what is important to industry	Director Infrastructure Coordination and Analysis, OIP
We trust USCG MSCs. How does OIC outreach fit with that?	Addressed to Director IC&A OIP
Govt has little understanding of the role/value of Ship Agents in MDA	Director of Field Ops, Moran Shipping
What we (govt) struggle with is knowing how you really operate and what you really do need, but also, when do I get you out of bed and say, “This is an issue?”	Panel Discussion 1
Government doesn’t have a clear understanding of how the industry works.	Panel Discussion 1
Classification	10
Trend to moving MDA under Intel shops in USN/USCG stifles sharing	Addressed to NMIC Director
Key initiative is eliminating Classification barriers	COPS Deputy Director
How are classification issues managed during OIP exercises?	Addressed to Director IC&A, OIP
Info sharing needs to be low-tech, unclassified and accessible	N3 Joint Ops Director, USFF
The culture of classifying MDA information needs to be eliminated	Chief of Security, BIMCO
OSAC declassifies information to be disseminated to a wider audience	Acting Director, OSAC
Problem arise when non-classified actors build on de-classified info and the government wants to use it – in a classified form	Panel Discussion 1
A way forward is two sets of architecture: one with open information sharing, the other for intelligence that doesn’t involve industry, unless it is so big it needs to be declassified and disseminated	Panel Discussion 1
The information flow for intelligence needs to be declassified and available in a central repository.	Manager, MAOC-D Lisbon
Are we going to protect intelligence sources through a "clearance" process for different stakeholders?	Manager, NZ National Maritime Coordination Center
Models for Success	8
The UK Chamber of Shipping's Project Camelot developed a matrix, including who should lead for different types of data.	Shipping Defence Advisory Committee, UK Chamber of Shipping
Success is based on confidence-building between partners, a simple cost structure, an inclusive approach, flag blindness, recognizing all UK shipping interests, and complementary approaches to other interests.	Shipping Defence Advisory Committee, UK Chamber of Shipping
establish bilateral linkages first; bilateral agreements have yielded better results than multilateral. Getting multiple players in a room together creates an environment in which the barriers come up.	Deputy Commancer, RSN Maritime Security Task Force
MAOC success: equal partnership, everyone has equal say, even if they do not have any intelligence to contribute on a particular issue.	Manager, MAOC-D Lisbon
Australia is using strategy of creating relationships with closest neighbors before reaching a little further out.	Breakout Topic 1 Discussion

ISSUE	OCCURENCES
Counter-drug community has ironed out many rough spots and produces actionable intelligence efficiently. Counter-terrorism community should take a step back and look to counter-drug as a model.	Breakout Topic 1 Discussion
If identified governments contribute personnel or equipment to a "coalition" sort of clearinghouse those people could perform the required research, sharing, and coordinating.	Manager, NZ National Maritime Coordination Center
The Amber Alert model is useful.	Panel Discussion 1
GMISS	8
Gatherings like GMISS are critical to defining Industry/Govt path forward	Deputy Secretary of Transportation
We are at GMISS to work through how industry provides information	Deputy Director, NMIC
GMISS is a good example of progress when it comes to information sharing, particularly rolling multiple conferences into one	Dir of Govt Relations, American Shipping & Logistics Group
While information sharing has much work to do, it is moving in the right direction because of events like GMISS	Senior Advisor – Intelligence, DHS
The concepts discussed at GMISS should translate into individual projects that can be tracked and accomplished.	Senior Advisor – Intelligence, DHS
Southeast Asia/Africa (Indian Ocean) Cooperative took six goals from GMISS to accomplish.	Panel Discussion 1
How can we have a GMISS without inviting representatives from the IMO, APEC, PMAESA, SPC, OAS, EU, WCO, IOTC, SAARPSCO, MARLO, and others?	Marine Security Operations Centre (East), RCMP
A simple commitment to maintain watch and answer queries will go a long way and be a major achievement from this conference to kick off global info sharing	Senior Enterprise Architect, ODNI
Vetted info vs. Immediate Info	8
The government wants information that is vetted and true to go out	Panel Discussion 1
The danger of instant information is that it is hard to make it accurate	Panel Discussion 1
I do need to trust the source. Then tell me what to do	Panel Discussion 1
LE: If you have an issue, you're putting it out early and often. Think: Virginia Tech.	Panel Discussion 1
There's a lot of operational information that must come out very quickly -- that we would like to have been able to keep our eyes open for immediately so we could do something about it.	Panel Discussion 1
If you put out the basic facts that you do have, private sector can feed information back as it develops.	Panel Discussion 1
Get something out there and let local experts help develop the picture.	Panel Discussion 1
Real time information on threats during London and Mumbai bombings was being updated rapidly and in real time on Wikipedia.	Panel Discussion 1
Anti-Piracy Capacity	8
Need to increase capacity to address piracy	Addressed to USCG Vice Commandant
Shared info is key to fighting piracy	Deputy Maritime Administrator
NIMC is a valuable new resource for fighting piracy	Deputy Maritime Administrator
We need to better understand the financing activities of pirates	Assistant Sec for Political Military Affairs, Dept of State
Need info sharing w/ industry to prosecute pirates	Assistant Sec for Political Military Affairs, Dept of State
The global legal system is failing to prosecute pirates	Addressed to Chief of Security, BIMCO
Use of LRIT allows ships under attack to continue to transmit their location	Panel Discussion 2
Having logistics in place before the hijack is critical, having codes set up between the crew and the ship owner so they can communicate effectively	CEO, Industrial Shipping Enterprise
TWIC Implementation	4
TWIC should be recognized universally by Fed	Addressed to USCG Vice Commandant
TWIC implementation in Baltimore (1st major port) was challenging	Deputy Secretary of Transportation
TWIC is a great example of a security measure that's not fully implemented	Deputy Secretary of Transportation
Ship/Port Agents could help make TWIC more effective	Director of Field Ops, Moran Shipping
MDA Silos	3
Building new silos in MDA	Addressed to USCG Vice Commandant

ISSUE	OCCURENCES
What I see happening is the opposite of the theme of this conference – increasing fragmenting of intelligence and increasing federalization.	Savanna Chief of Police
Not only are there national, regional, etc. stovepipes, but now we see functional stovepipes just focusing on drug interdiction, piracy, etc.	Breakout Topic 1 Discussion
Civil Liberties	3
How do you expand dissemination without stepping civil rights and civil liberties?	Senior Advisor – Intelligence, DHS
DOJ SAR standardizes reporting and protects civil liberties.	Civil Liberties Protection Officer, ODNI
National security/civil liberties balance metaphore is not necessarily true: securing the data better is beneficial for all parties.	Civil Liberties Protection Officer, ODNI

Appendix F
GMISS Working Group
Common Conclusions

GMISS Working Group Points of Discovery				
	Working Group A	Working Group B	Working Group C	Working Group D
Issue	Building a global maritime information exchange grid	Bridging the understanding gap between maritime industry and government	Resolving Information Privacy, Proprietary & Classification	Building on piracy as a model of co-developed, mutually beneficial policies
Government and the maritime industry need improved mutual understanding		Agreed		Agreed
Need trusted single point of contact to push classified & non-classified information in usable form between industry and government			Agreed	Agreed
Need international maritime information sharing governance structure w/ clear objectives and goals	Agreed			Agreed
Need industry/NGO/internatinal governmental representation at information sharing discussions	Agreed			
Existing non-classified web portals can make info available	Agreed			
Meta-site can link portals with feedback	Agreed			
Need panel to identify what information is needed	Agreed			
Need access controls	Agreed			
Current inaction (specifically re. piracy info sharing) displays a lack of resolution on the part of many nation states				Agreed
The current anti-piracy collaboration model has far too many constraints and complexities – politically, economically and tactically.				Agreed
The co-ordination of industry and the military, i.e. SHADE, is a paradigm for future use to create safe shipping				Agreed
Enhanced co-ordination established between industry and the military should not be lost				Agreed

Issues in bold text were addressed by multiple working groups, as indicated by highlighted cells. Blank cells indicated this issue was not addressed by this working group.

GMISS Working Group Actionable Items				
	Working Group A	Working Group B	Working Group C	Working Group D
Issue	Building a global maritime information exchange grid	Bridging the understanding gap between maritime industry and government	Resolving Information Privacy, Proprietary & Classification	Building on piracy as a model of co-developed, mutually beneficial policies
Develop meta site linking existing infrastructure to share info; consolidate AIS sharing systems	Agreed		Agreed	
Evaluate existing mutual training, identify gaps and institute needed additional training.		Agreed		Agreed
Non-government organization manage international governance options for Global AIS			Agreed	
Develop a single point of contact for maritime crises				Agreed
Build on the response models created by UKMTO and the SHADE group				Agreed
Define the "as is" state of the "global grid"	Agreed			
Create a panel to define what information is needed by whom	Agreed			
Develop training for information sharing professionals			Agreed	
Establish a uniform U.S. Government policy mandating interagency information sharing and outlining dispute resolutino proceedures			Agreed	
Industry participate in the U.S. Maritime Domain Awareness Stakeholder Board		Agreed		
Industry participate in the U.S. MSIPC by inviation		Agreed		
Expand America's Waterway Watch program to encompass all users			Agreed	
Develop and implement a global marketing plan for government/industry/NGO maritime info sharing	Agreed			
Share best practices in maritime security in a common environment to drive future development of industry standards				Agreed

Blank cells indicate the issue was not addressed in this working group

Issues in bold text were addressed by multiple working groups, as indicated by highlighted cells. Blank cells indicated this issue was not addressed by this working group.

GMISS Working Group Ongoing Discussion Points and Recommendations				
	Working Group A	Working Group B	Working Group C	Working Group D
Issue	Building a global maritime information exchange grid	Bridging the understanding gap between maritime industry and government	Resolving Information Privacy, Proprietary & Classification	Building on piracy as a model of co-developed, mutually beneficial policies
Who can use a global grid?	Agreed			
Identify the information requirements	Agreed			
Are there existing meta sites?	Agreed			
Are we going to review information out there to make sure there is not duplication of information/efforts?	Agreed			
Need simple, one time log-on for entire grid	Agreed			
Review the regulations to determine if there's overlap and/or archaic regulations		Agreed		
Next GMISS this working group explore intermodal operations and regulatory issues surrounding MDA		Agreed		
Invite MTSNAC/CMTS to GMISS		Agreed		
Need continuing involvement of agencies industry most interacts with, such as USCG and CBP		Agreed		
Government needs to limit impact of information reporting on industry operations			Agreed	
Industry needs protection from retribution for credible reporting			Agreed	

Issues in bold text were addressed by multiple working groups, as indicated by highlighted cells. Blank cells indicated this issue was not addressed by this working group.

Shared Priorities Inferred from GMISS Working Group Combined Results: Pending Working Group Approval				
	Working Group A	Working Group B	Working Group C	Working Group D
Issue	Building a global maritime information exchange grid	Bridging the understanding gap between maritime industry and government	Resolving Information Privacy, Proprietary & Classification	Building on piracy as a model of co-developed, mutually beneficial policies
Identify and empower an NGO, with industry/government/NGO representation, to lead development of a global maritime info sharing grid, establish standards, consolidate systems, identify requirements, link existing sites and neworks; and to provide dispute resolution between conflicting interests.	Agreed	Agreed	Agreed	Agreed
Identify a single point of contact to coordinate maritime awareness/MDA development issues between U.S. government and maritime industry	Agreed		Agreed	Agreed
Assess current mechanisms for developing mutual understanding between industry and government, promote these opportunities to all members of the GMCOI, develop plan to fill gaps.		Agreed	Agreed	Agreed
Identify a single trusted point of contact to manage ongoing information flow between industry and U.S. government, including tip reporting, collorative awareness and intelligence development, threat warnings, and other alerts.		Agreed	Agreed	Agreed
Establish or identify regional centers to manage ongoing information flow among all stakeholders in their area of operations; form a board comprised of these regional entities to coordinate global flow of maritime information, under international maritime information sharing governance structure w/ clear objectives and goals.	Agreed		Agreed	Agreed

Inferred priorities were compiled based on issues addressed by working groups as indicated by highlighted cells. Blank cells indicated this issue was not addressed by this working group.

Appendix G
GMISS 2008 Executive Summary

Global Maritime Information Sharing Symposium 2008

"*...trust and cooperation cannot be surged. They must be built over time so that the strategic interests of the participants are continuously considered while mutual understanding and respect are promoted.*" Cooperative Strategy for 21st Century Sea Power.

"*Overcoming cultural and policy barriers to information sharing requires changes in business practices and information security procedures*." National MDA CONOPS.

"*….we understand that our success depends on a strong foundation of partnership with our maritime stakeholders,*" Rear Adm. James Watson, Coast Guard Director of Prevention Policy.

Executive Summary

The inaugural Global Maritime Information Sharing Symposium (GMISS) was held on August 20-21, 2008 at the U.S. Merchant Marine Academy (USMMA) in Kings Point, New York and brought together a diverse mix of over 125 participants from maritime companies, associations, navies, coast guards and government agencies from around the world.

GMISS is designed to be an annual symposium over the next five years, sponsored in conjunction with the U.S. Maritime Administration (MARAD) and under the auspices of the Commercial Outreach/Private Sector Working Groups of the National Maritime Domain Awareness (MDA) Stakeholder Board. It is dedicated to enhancing the information sharing relationships between the Maritime Industry and the U.S. Government (USG) through the coordination of the Office of Global Maritime Situational Awareness (OGMSA).

Why GMISS?

The symposium supports the Maritime Administration in developing a coherent federal outreach and coordination effort. Leading up to this symposium, the U.S. Navy (USN) and U.S. Coast Guard (USCG) had expressed the need to expand their relationship with industry as set forth in the Cooperative Strategy for 21st Century Seapower. As government agencies have increasingly realized the benefits to be gained by partnering with the maritime industry however, there has been a flurry of "commercial outreach" and a deluge of information requests that are overwhelming industry and rapidly eroding its eagerness and ability to respond. The maritime community, both directly and through its various associations, has expressed frustration and confusion over the seemingly uncoordinated efforts in support of and demands being place on maritime trade and security by government entities.

The GMISS was undertaken as an effort to harness this government energy for engagement and establish a means to coordinate a more cohesive dialogue between government and maritime industry representatives. GMISS is an opportunity to demonstrate that a USN/USCG/MARAD partnership can open the doors of communication to further advance the maritime strategy, and equally, begin to provide the coordination necessary to present a unified voice to the maritime community.

The long range (multi-year) objectives of the GMISS include:

- Coordinate the U.S. Government's maritime commercial outreach
- Implement industry/government working groups
- Highlight specific government relationships
- Promote regional involvement
- Engage a diverse range of stakeholders

Through an "issue–to-working-group" progression in this inaugural GMISS and reflecting the needs of this inaugural symposium's main sponsors (OGMSA, Department of Justice "COPS", USFF/NCAGS and MARAD), the broad topic that is open maritime data sharing was approached from three particular vantage points:

- Law Enforcement Information Sharing in the Maritime Environment (The Evolution of Fusion Centers and Information Sharing with Law Enforcement).
- Regional Blue Water Information Sharing (Increased understanding and liaison with commercial shipping).
- Industry and Maritime Information Sharing (Increased understanding and data sharing with the commercial maritime industry).

Symposium attendees were asked to formulate their thoughts around five core questions:

- How can the U.S. Government be more coherent in its approach to the Maritime Industry?
- What should be the model for information sharing between the U.S. Government and the Maritime Industry?
- What are the unexploited maritime information sharing opportunities that will benefit the flow of commerce and help trade?
- How do we leverage the national strategy for maritime domain awareness to further these efforts?
- Is there value in continuing an annual symposium such as GMISS as the center of focus for issues and innovations?

This combination of vantage points and core questions was focused in four working groups, each addressing a specific issue. These issues had been developed during OGMSA's work with such maritime associations as the World Shipping Council, the Cruise Line International Association (CLIA), and numerous individual industry representatives.

- Working Group A: Issue - Can Government Information Requests to Shipping Companies be Consolidated, Streamlined, Standardized or Reduced?
- Working Group B: Issue - What is the Law Enforcement/Industry Model for an International/Domestic Maritime Information Sharing Center?
- Working Group C: Issue - What does the Maritime Industry Want from the World's Navies and Coast Guards?
- Working Group D: Issue - How do we Create Economic Incentives for Maritime Information Sharing?

Working Group Findings

Consolidated summary findings as generated from the symposium's four independent working groups can be summarized into the following eight categories and potential courses of action:

- Inventory: Establish baseline maritime information requirements (both government's and industry's).
- Cost/benefit: Determine the cost of providing information that is requested or required versus its intended and real benefits.
- Standardize: Standardize the requested information and the procedures for its exchange, globally.
- Portals/Hubs: Set up commercially-based "portals/hubs" through which maritime data can be centralized/exchanged.
- Incident Exchange: Set up a global incident information exchange for use by industry/navy/coast guards.
- Market: Market all the above broadly across industry/government/navy/coast guards to ensure broadest involvement from all possible stakeholders.
- Acta non verba: (i.e. these issues have been discussed enough, let's make them happen).

A summary of individual working group discoveries and action items can be found in the Attachment section of this report.

Conclusion

The concept behind GMISS and its inaugural symposium appear to have been well received by both industry and government attendees as expressed by their subsequent comments and of greater importance, by the significant number of industry attendees volunteering to continue to participate in the working groups.

The symposium topics set forth through the symposium agenda, outlined via plenary and break-out presentations and then refined to issues through working groups also appear to be along the same lines as those being wrestled with at the various USG inter-agency MDA meetings of which OGMSA has been a part.

Further, a rough preliminary comparison of the GMISS outcomes with the materials from other USG commercial outreach symposium efforts (see attachments) indicates a parallel trend of issues being brought forth by industry participants regardless of venue including:

- The need for USG to speak a singular MDA message.
- The need for a coordination of USG maritime information requests of industry.
- The need for a single portal to send requested data to for subsequent internal USG distribution
- The need for a cost/benefit analysis of data being requested or required.
- The need for reciprocity on data requests.
- The need for action towards mutually beneficial solutions.

Regardless, while the momentum created by GMISS and other such events has been positive, post-symposium actions are of greater importance lest GMISS becomes yet another USG conference gathering data from industry but not making any changes as a result.

It is the crucial need for post-conference actions that prompted this report and its recommendations.

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

Appendix H
2009 MIST (Puget Sound)
Executive Summary

Executive Summary

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

About MIST

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

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

Figure 1: the MIST Process

Executive Summary

Our findings

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

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

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

The Puget Sound is driven by economics and safety

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

Financial and Operational Incentives

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

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

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

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

John does safety, security and operations

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

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

Executive Summary

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

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

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

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

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

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

Executive Summary

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

Recommendations

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

Good communication is key

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

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

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

Recommendations

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

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

Profile of an FSO
Information needs

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

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

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

Executive Summary

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

Information should be easy to access and of high quality

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

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

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

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

Recommendations

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

MIST should provide value and be sustainable

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

Executive Summary

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

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

Recommendations

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

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

GLOBAL MARITIME INFORMATION SHARING SYMPOSIUM

GMISS

www.gmsa.gov/gmiss