Area Maritime Security Committees

Challenges, Accomplishments, and Best Practices

2016 Annual Report

U.S. Coast Guard

Washington, D.C.

November 1, 2017

Contents

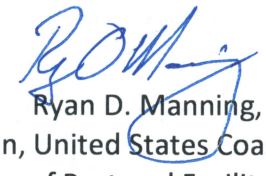
Office Chief's Perspective

Area Maritime Security Committees (AMSCs) are the cornerstones in bolstering the lines of defense of our Nation's ports. Their importance cannot be over emphasized. Collaborative planning, coordination, open lines of communication, working relationships, and unity of effort are essential to providing layered security and effective measures across all segments of the Marine Transportation System (MTS).

The maritime industry is a dynamic industry that includes many components. It provides vital transportation along marine highways, enables the harvesting of marine and offshore natural resources, supports recreation, and facilitates interstate and international trade. By providing access to transportation, trade, and natural resources, the maritime industry supports our nation's economic prosperity and is a key driver for our national economy.

Increasing demands on the MTS create additional operational risks that must be managed to ensure the MTS continues to serve as an engine of the American economy. AMSCs support the Coast Guard's efforts to develop common-sense security policies and regulations in the maritime domain and provide crucial advice in the way field commanders apply those policies to provide the maritime industry consistency in their business models. This provides industry greater incentives to invest wisely and drive the MTS forward, thus sustaining and improving the national economy and American prosperity.

I am pleased to publish this report that shows the unparalleled work our partners in the AMSCs are doing and highlight the successes that over 13 years of close public/private partnerships have brought. As we strive for continual improvement in the way we do business, I value the feedback from our Port Security Specialist community, as the executer's of the policy we strive to provide you. In fact, the resurrection of this consolidated report is due to interest expressed by your community to provide a readily available document that tells the story across all of our 43 AMSCs.



Ryan D. Manning,
Captain, United States Coast Guard
Chief, Office of Port and Facility Compliance

1.0 Background

The implementation of the Maritime Transportation Security Act of 2002 (MTSA) mandated the establishment of regional Area Maritime Security Committees (AMSCs) as collaborative forums for government and industry partners to work together to enhance security in the maritime environment. This is accomplished through meetings, partnerships, networking, information sharing, training, vulnerability assessments, and development of plans and strategies. The local AMSC annual reports are an important tool used to compile and share information pertaining to AMSC issues such as: committee organization, training events, challenges, accomplishments, best practices, and recommendations. These efforts ensure the Coast Guard and the maritime communities maintain alignment with national preparedness goals, strategies, and reporting requirements, and ultimately serve to improve AMSC effectiveness nationwide.

The following information was collected from the 2016 annual reports of local AMSCs.

2.0 Challenges

AMSCs were asked to identify specific challenges or impediments that may have been encountered in 2016. Enclosure (1) identifies all challenges reported in the 2016 annual reports. The reports highlighted several common challenges:

Cyber Risk Management and the Marine Transportation System (MTS). Cyber risk management is a rapidly evolving area of concern and indeed a growing activity for AMSCs. Many Captains of the Port/Federal Maritime Security Coordinators (COTP/FMSCs) have established AMSC Cyber subcommittees to aid in addressing cyber risk, information sharing, and resiliency within their ports and shared stakeholders. However, other than raising awareness through the AMSC, COTP/FMSC's continue to experience limited expertise and training to address cyber risks within the MTS. Continued collaborative development and refinement of national guidance and policies clarifying the AMSC's expected role in safeguarding the cyber aspect of MTS critical infrastructure will be greatly beneficial to the AMSCs. Additionally, efforts should continue to increase field unit cyber-related knowledge to apply actionable measures used to assess the cyber threat within the MTS with possible solutions to mitigate risk, including up-to-date training.

AMSC Management Funds. Districts continue to praise the supplemental AMSC management funds provided by The Office of Port and Facility Compliance (CG-FAC) over the past 10 years. Although a positive initiative, recent budget reductions have eliminated the availability of supplemental funding and are having an impact on the COTP/FMSCs ability to conduct additional AMSC activities, particularly in those Sectors with large geographic areas operating under several established AMSC Regional Subcommittees. AMSCs recommend supplemental funding be reestablished as soon as possible pending solutions to budgetary challenges.

3.0 Accomplishments

The AMSCs are forums for coordination of security related issues and partnerships in U.S. ports. Their collaborative efforts strengthen cooperation among stakeholders. In 2016, AMSCs conducted 671 meetings, 332 Joint Agency training meetings, 189 Maritime Security training events and conducted 45 training exercises nationwide. These coordination and collaboration opportunities have resulted in effective, real world security prevention, response, and recovery efforts. Enclosure (2) identifies accomplishments reported in the 2016 annual reports.

The following figures highlight AMSC training efforts nationwide.

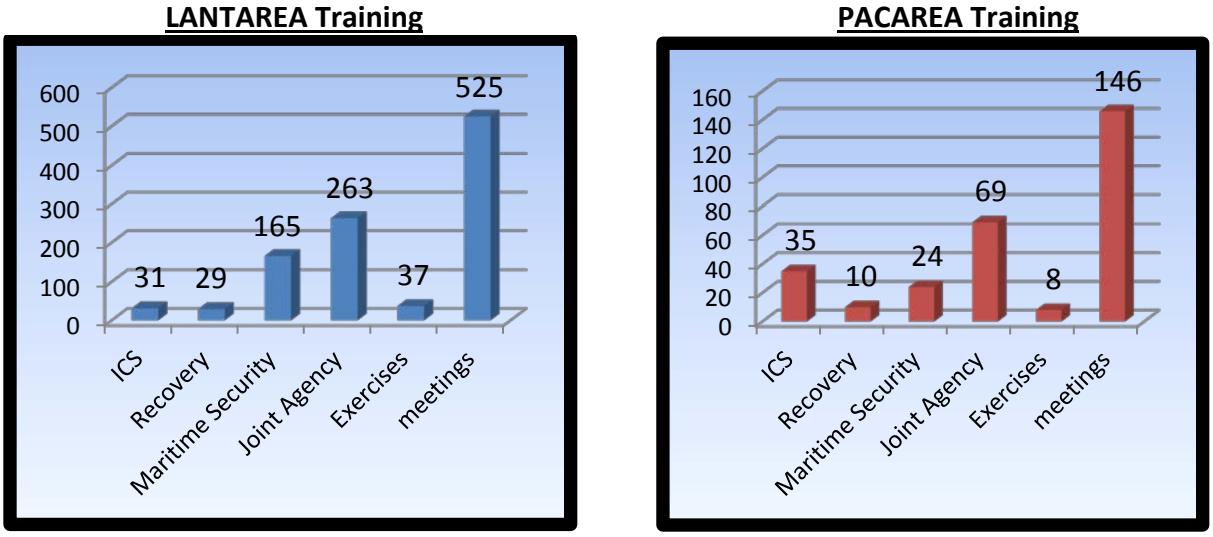


Figure 1 - AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners/stakeholders that do not fall into the ICS, Recovery, Maritime Security, Exercises or Meetings categories; Exercises include all tabletop exercises and drills; Meetings are tallied up from all AMSC's in each respective area.

Cyber security is an increasing activity under discussion by COTP/FMSCs and their AMSCs. Capitalizing on what's already been learned and implemented within the physical security domain, the AMSC's will continue to evolve and be able to understand how to use and interpret standard processes and assessment tools that will provide the means to enhance prevention, response, and recovery from cyber-related incidents within the MTS.

Additionally, AMSCs incorporated Radiological/Nuclear (RAD/NUC) Detection Regional Concept of Operations (CONOPs) and Standard Operating Procedures (SOPs). DHS's Domestic Nuclear Detection Office (DNDO) was instrumental in developing RAD/NUC CONOPs & SOPs for numerous PACAREA and LANTAREA COTP/FMSCs and their AMSCs. The RAD/NUC CONOPs & SOPs were included as an Annex within the AMSP and some were exercised under the Area Maritime Security Training and Exercise Program. AMSCs were instrumental in the planning and coordination of effort involved in the development of this AMSP Annex, including

collaboration between port stakeholders, and the planning facilitators from DNDO and the Oak Ridge National Laboratory.

The AMSCs were also involved in projects that provided increased security within their respective port areas. Some examples of these projects include:

Cooperation and support of the Commonwealth's initiative to develop a Preventive Radiological Nuclear Detection (PRND) CONOPs and SOP: The Boston AMSC cooperated with the Commonwealth of Massachusetts's initiative to develop a statewide PRND CONOP and SOP similar to the maritime PRND CONOPs/SOP completed in 2014. With support from DNDO and the Department Of Energy, the Commonwealth embarked on this important initiative and held many meetings throughout the year. Boston AMSC and the Boston RND Permanent Advisory Group attended almost all of these meetings offering support and input. The CONOPs and SOP were recently adopted and planning is now underway to exercise those documents. This initiative, when paired with the Maritime PRND CONOPS/SOP, will provide state-wide coverage.

Small Vessel Preventive Radiological and Nuclear Detection (PRND) Initiative: The Puget Sound AMSC Small Vessel PRND Initiative, funded by a Port Security Grant, brings together 32 regional State, Local, Tribal, and Federal agencies working in concert to provide PRND screening as a secondary mission during maritime operations, and to assist in 100 percent screening operations when warranted. Regional partners continue to conduct quarterly "on the water" drills and initial/follow-on training for personnel at least once a year.

4.0 Best Practices

The AMSC reports identified many helpful and practical best practices. Below are highlights of specific programs, concepts and initiatives. Enclosure (3) identifies best practices reported from each AMSC in 2016:

Partnership with the Transportation Security Agency (TSA) in application of Visible Intermodal Prevention and Response (VIPR) teams: Sector Long Island Sound AMSC partnered with TSA in application of VIPR teams to leverage resources quickly and to increase and augment security at intermodal nodes (such as at large Ferry operations) and during large scale marine event public gathering events. Typically VIPR teams are comprised of a myriad of law enforcement entities and stakeholders, along with USCG and federal participants. Port Security Grant funding of local partners to participate in VIPR operations resulted in a significant force multiplier and increased effectiveness. VIPR team participants are trained and equipped with PRND resources, which can detect medical and industrial radiation or nuclear material. VIPR teams have the capability to isolate and identify radiological materials which can be utilized in constructing or introducing small, portable nuclear devices such as "dirty bombs" into transportation systems. These capabilities at the local level are critical to their PRND CONOPs.

AMSP Geographic Information System (GIS) Integration: Sector New York integrated aspects of their AMSP into GIS, which was incorporated into New York City's Office of Emergency Management's Maritime Emergency Transportation Plan. This information will provide a broader understanding to State and Local Partners of the critical infrastructure within Sector New York.

Seattle Pacific Northwest Maritime Fusion Group: Jointly chaired by Coast Guard Sector Puget Sound, FBI Seattle, and the Naval Criminal Investigative Service (Northwest Field office), the Seattle Pacific Northwest Maritime (SPAM) Fusion Group is a Maritime Counter Intelligence/Counter Terrorism resource directly supporting the COTP and the AMSC Executive Committee. The SPAM is instrumental in providing maritime intelligence briefings to the senior leadership of the Executive Committee at a classified level and sensitive security information (SSI) briefings to general committee members that meet "covered person" and "need to know" criteria. Under the Regional Coordination Mechanism (ReCoM), the SPAM collaborates with other DHS members and local agencies providing intelligence and information sharing as well as training/exercises and maritime risk evaluation. The ReCoM Council is directly linked with the AMSC Executive Committee. The SPAM exists as the multi-agency intelligence subcommittee of the AMSC. As such, the AMSC shares information and intelligence, assesses threats, and disseminates reporting as needed to the AMSC.

5.0 Emerging Security Issues

Ensuring security and resilience in the MTS is an ever evolving challenge necessitating the close collaboration of MTS stakeholders in forums such as AMSCs. Looking ahead, the AMSC network will provide a critical framework to address emerging challenges in the maritime domain including issues such as:

Cyber:

Cyber systems are an integral part of the nation's critical infrastructure, and are vital to the nation's economy and security. Both the public and private sector are increasingly dependent on cyber systems for both routine and emergency services. Like other systems, cyber systems are vulnerable to accidents, natural disasters, and deliberate attacks. Cyber systems also have unique vulnerabilities, many of which are not apparent to the casual user, and are subject to accidental or intentional acts that may originate far from the impacted area.

Since the signing of the Coast Guard's Cyber Strategy, CG-FAC remains the lead office for implementing the Protect Infrastructure portion of the Strategy. One significant milestone CG-FAC has achieved towards critical infrastructure protection is the completion of the draft Cyber Navigation and Vessel Inspection Circular that was released via the Federal Register on July 12, 2017 for public comment.

The Coast Guard, working with the Department of Transportation (DOT) and TSA, developed

Enhanced Coordination Procedures (ECPs) in accordance with directives outlined in Presidential Policy Directive 41 (PPD-41), titled "United States Cyber Incident Coordination." PPD-41 was published on July 26, 2016 and defines what constitutes a significant cyber incident and more importantly, who is responsible for responding to a significant cyber incident. ECPs are designed to enhance unity of effort and ensure that consistent response procedures are developed, deployed, and updated as appropriate.

Finally, the Coast Guard worked with the National Institute of Standards and Technology (NIST) and maritime industry stakeholders to develop the voluntary Cybersecurity Framework (CSF) Profile for Maritime Bulk Liquid Transfer (MBLT) facilities, which was released in November 2016. The MBLT Profile serves to assist in conducting cybersecurity risk assessments for those entities involved in MBLT operations overseen by the USCG. It is intended to act as non-mandatory guidance to organizations conducting MBLT operations within facilities and vessels under the regulatory control of the USCG via the Code of Federal Regulations (CFR) 33 CFR 154-156. The Coast Guard is in the process of developing two additional CSF Profiles that focus on offshore (oil and gas) and passenger operations. It is anticipated these two CSFs will be published late 2017/early 2018.

MTS Resilience/Recovery:

CG-FAC continued to advance Marine Transportation System (MTS) Recovery concepts and policy throughout the year. The Security and Accountability For Every Port Act of 2006 (SAFE Port Act, Pub. L. 109-347) requires the inclusion of MTS recovery protocols in Area Maritime Security Plans (AMSP). The development of AMSPs is an AMSC responsibility. In order to create and apply resiliency and recovery concepts in all-hazard scenarios a working group comprised of CG-FAC, Area, and Sector personnel was established to draft a Navigation and Vessel Inspection Circular (NVIC) that provides comprehensive guidance on the development of stand-alone MTS recovery plans. The NVIC should be available to AMSCs and their partners in late 2017 or early 2018. In addition, field unit personnel attending the Facility Inspector/Port Security Specialist (FI/PSS) workshop provided valuable recommendations to update the MTS Recovery policy and Common Assessment and Reporting Tool (CART) guidance and User's Guide.

The Cascadia Rising 2016 Exercise, which evaluated Federal, State, Local, Tribunal and maritime industry stakeholder response to a 9.0 magnitude earthquake and resulting tsunami along the Pacific Northwest's Cascadia Subduction Zone, identified needed additional regional MTS Recovery response updates. Additionally, CG-FAC provided MTS Recovery expertise to senior leaders in response to any threats that impact movement of commerce on the nation's waterways during the Federal Emergency Management Agency's (FEMA) National Exercise Program Capstone Exercise 2016.

In October 2016, Hurricane Matthew required maritime stakeholders from Florida to Virginia to prepare for and potentially respond to a MTS disruption along the Southeast Coast. National planning for Matthew included identifying Coast Guard Port Security Specialist and Port Recovery Specialists from outside the impacted area to prepare for deployment in support of MTS Recovery operations at affected units and coordinating with Customs and Border Protection (CBP) and DOT personnel managing the FEMA Emergency Support Function One (ESF-1) response. CBP and CG-FAC also updated the CBP/CG Joint Protocols for the Expeditious Recovery of Trade to reflect current CBP and CG leadership, the Communications Flow Chart, and the Protocol Participation Matrix.

There are several upcoming initiatives impacting MTS Recovery concepts and policies in 2017. Updates to the CG MTS Recovery Instruction and CART User's Guide are scheduled to be completed and promulgated that will address recommendations from field units and lessons learned from real world events. These policy updates will be discussed at future contingency planning, FI/PSS, and MTS Recovery workshops. CG-FAC will continue discussing MTS Recovery planning and coordination with CBP, DOT ESF-1, and FEMA counterparts during national level exercises and real world events. Those agencies represent important federal partners in MTS recovery and the updated policies reflect continued partnerships.

Cyber risk management and impacts of a cyber incident to the MTS continues to be an area of great importance to the CG. The rapid evolution of cyber technology has a substantial impact on the MTS in terms of efficiency and cyber risks. Upon the promulgation of cyber policies for facilities and vessels, MTS Recovery instructions and policies, and the MTS Recovery Plan will be updated as necessary to comply with any new requirements. CG-FAC will continue to support field units in response to significant MTS disruptions, particularly during hurricane season.

6.0 Conclusion

Maritime security is at the forefront of the United States ports and waterway infrastructure security posture. The AMSCs are an integral part of the maritime security regime and must continue to evolve and adapt accordingly to combat emerging threats while ensuring the unimpeded flow of commerce. Security challenges, whether physical or cyber related, remain a constant fixture and continue to pose potential adverse impacts to our critical Marine Transportation System. Continued collaboration, information sharing, and coordination via AMSCs are vital to mitigating risks and essential to the efficient facilitation of commerce.