Area Maritime Security Committee

Challenges, Suggestions, Accomplishments, and Best Practices

2018 Annual Report

U.S. Coast Guard

Washington, D.C.

Contents

Office Chief's Perspective

Authorized from the enactment of the Maritime Transportation Security Act (MTSA) of 2002, Area Maritime Security Committees (AMSCs) have served as an incredibly valuable focal point for regional collaboration to enhance maritime security at the port level. These committees unite the wide array of maritime stakeholders who share a common interest in ensuring the preservation of a secure and resilient Marine Transportation System (MTS). The 43 AMSCs are led by their local U.S. Coast Guard Captain of the Port (COTP)/Federal Maritime Security Coordinator (FMSC).

The Marine Transportation System (MTS) is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports, supports $5.4 trillion dollars of economic activity each year, and accounts for the employment of more than 30 million Americans. Any significant disruption to the MTS, whether man-made or natural, has the potential to cause cascading and devastating impacts to our domestic and global supply chain and, consequently, America's economy and national security. AMSCs are comprised of subject matter experts from Federal, Territorial, Tribal, State, and Local agencies as well as public and private port stakeholders to ensure the safety, security, and resilience of our nation's critical MTS.

The AMSC Annual report serves as an immensely valuable resource for sharing of information amongst the entire national AMSC network. The transparent sharing of challenges, suggestions, accomplishments and best practices is vital for enhancing national maritime security. The AMSC framework embodies the Coast Guard's priority of unity of effort through the establishment and sustainment of port partnerships as they continue to address emerging threats and issues that have the potential of impacting the maritime domain.

Bradley W. Clare,
Captain, United States Coast Guard
Chief, Office of Port and Facility Compliance

1.0 Background

The implementation of the MTSA of 2002 mandated the establishment of regional 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. Local AMSC annual reports are an important tool used to compile and share information pertaining to AMSC issues such as committee organization, training, challenges, accomplishments, best practices, and recommendations. These efforts ensure the Coast Guard and the maritime communities maintain alignment with national preparedness goals, strategies, reporting requirements, and ultimately serve to improve AMSC effectiveness nationwide.

2.0 Challenges

AMSCs identified specific challenges or impediments encountered in 2018. Enclosure (1) identifies all challenges reported from each AMSC in 2018. The following highlight common challenges:

Cybersecurity and the MTS. The dynamic nature of cybersecurity threats and the shortage of subject matter experts in government and industry make cybersecurity preparedness, response and recovery a continuing challenge as noted in the 2018 reports. One AMSC said it was difficult to harmonize Coast Guard Cyber Strategy in a linear port-wide system with limited influence over non-MTSA operations. The reports also highlight a concern in reference to stakeholders applying for Port Security Grant Program (PSGP) funding to initiate cybersecurity projects due to the limited guidance on cyber, and the lack of in depth field knowledge to properly assess the cybersecurity investment justifications during the PSGP field review.

Unmanned Aircraft Systems (UAS) access to the MTS. The increased frequency and reporting of UAS intrusion over MTSA-regulated facilities is generating questions and concerns from Facility Security Officers and other security personnel. Another report identified a concern that security zone regulations do not extend to the air space in regards to transiting cruise ships and escorted vessels. Other mechanisms for enforcement and mitigation of the associated risks still need to be addressed.

Homeport 2.0. Homeport is an internet portal utilized by the Coast Guard to support secure information sharing requirements as per MTSA and provide information about the Coast Guard's primary missions to the public. Homeport facilitates the sharing of information between Coast Guard personnel, members of the maritime community, and other designated port stakeholders. Homeport functionality continues to be a challenge for management of accounts for members and the ability to effectively communicate to the maritime stakeholders. AMSC members are discouraged from using the Homeport enterprise system due to the difficulty in maintaining access and the multiple error messages that they encounter as they attempt to navigate in the current system.

Port Security Specialist (PSS) expansive responsibilities. A number of AMSCs stated they did not have a Security Specialist (Recovery) billet to address the new Marine Transportation System Recovery Plan (MTSRP) template that was introduced in NVIC 04-18. This further increased the workload for PSSs. The workloads have increased since the inception of the PSS billets potentially impacting relationships with local communities and port partners. The PSS may not be able to participate in state and local exercises and attend state and local security related committees due to the number of assigned missions (e.g., AMSC management, AMSP maintenance, Area Maritime Security Assessments (AMSAs), Area Maritime Security Training and Exercise Program (AMSTEP) Exercises, manage Homeport, Alert Warning System-Port Partners [AWS-PP], Maritime Security Risk Analysis Model [MSRAM], PSGP, etc.). Ongoing challenges affecting the PSS workforce are declines in funding and increased workloads.

Maintaining AMSC Membership. AMSC members volunteer their time and effort without compensation or travel/per diem support. Port recovery planning, exercise participation, annual port risk assessments, grants management, and Homeport create an increasing burden on the volunteer port community. With much of the MTSA program reaching maturity, meetings are becoming more focused on Coast Guard and non-security issues, such as navigation and shared waterway use. AMSCs continue to struggle with nurturing the high level of interest needed to maintain a vibrant port security program.

Active Shooter (AS)/Active Threat (AT). AMSCs have started to stand up AS/AT subcommittees. A common concern was the level of training, the type of gear, and weapons needed to respond to an AS/AT incident in the maritime domain.

3.0 Suggestions

The AMSC reports identified many helpful and practical suggestions. Below are highlights of specific programs, concepts, and initiatives. Enclosure (2) identifies suggestions reported from each AMSC in 2018:

Cybersecurity/Cyber Risk Management. AMSC cyber subcommittees must continue to foster an open information sharing environment for port partners and leverage the available subject matter expertise to highlight critical nodes and identify existing cybersecurity vulnerabilities. The Coast Guard should continue to seek funding for cybersecurity training and expertise to meet these challenges. One AMSC suggested CG-FAC coordinate with DHS-Cybersecurity and Infrastructure Security Agency (CISA) to procure and incorporate cybersecurity grant funding to port areas responsible for AMSP development. Cybersecurity training should be tailored for AMSC members that increases awareness of cybersecurity issues and ways to mitigate cyber vulnerabilities.

Homeport 2.0. A recurring suggestion from field units is to tailor Homeport 2.0 to meet or exceed the functionality of Homeport 1.0. Job aids and training materials need to be developed specifically for AMSC Executive Secretaries and end users. COTPs should have permissions to

approve port stakeholder registrants in their area of responsibility and to reset passwords when needed.

UAS. AMSCs recommend Coast Guard Headquarters work with DHS to engage Federal Aviation Administration (FAA) on the legal and policy challenges to fielding counter-UAS systems. One recommendation was for Coast Guard and Department of Homeland Security (DHS) to support acquisition of UAS capabilities for federal, state, and local law enforcement and emergency response agencies through direct appropriations and appropriate grant program prioritization. Additionally, they suggested the Coast Guard and DHS support the creation of techniques, tactics, and procedures for interoperability and information sharing to improve situational and domain awareness to reduce risk in the port environment.

Active Shooter (AS)/Active Threat (AT) Incidents: AMSCs suggest that CG Headquarters update or expand policy guidance in reference to AS/AT incidents. Training and proper equipment to meet policy requirements needs to be addressed. AMSCs recommend passenger vessel crews need specific training and guidance to address AS/AT Threats.

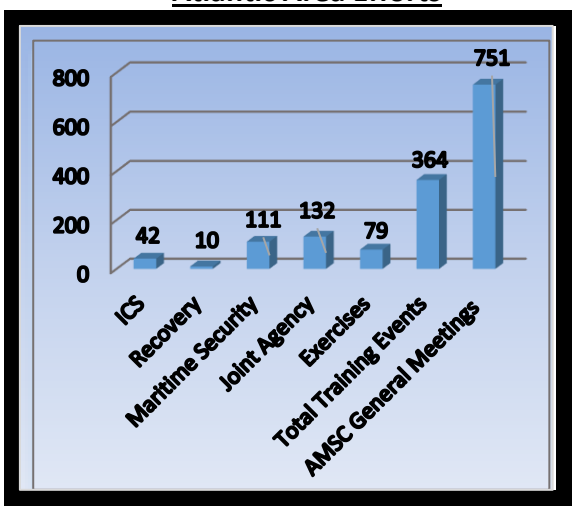
AMSC Support Funds: AMSCs recommended restoration of supplemental funds in support of activities within the COTP Zone. Additionally, it is recommended that funding be identified for restoration of a national conference or event to be held for AMSC leadership. This provides for crucial collaboration time with Committees from around the nation, and facilitates the employment of best practices as shared in these reports.

4.0 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 2018, AMSCs and their respective subcommittees collectively facilitated 1,335 events. This total included 895 administrative AMSC meetings (e.g., Executive Steering Committees and General AMSC meetings) and 440 training specific events (includes 144 Joint Agency training meetings, 118 maritime security training operations, 100 training exercises, 73 Incident Command System training sessions and 15 MTS Recovery Unit training sessions). These coordinated opportunities resulted in effective, real world security prevention, response, and recovery efforts. Enclosure (3) identifies accomplishments reported from each AMSC.

The following tables highlights AMSC efforts nationwide:

Atlantic Area Efforts



Pacific Area Efforts

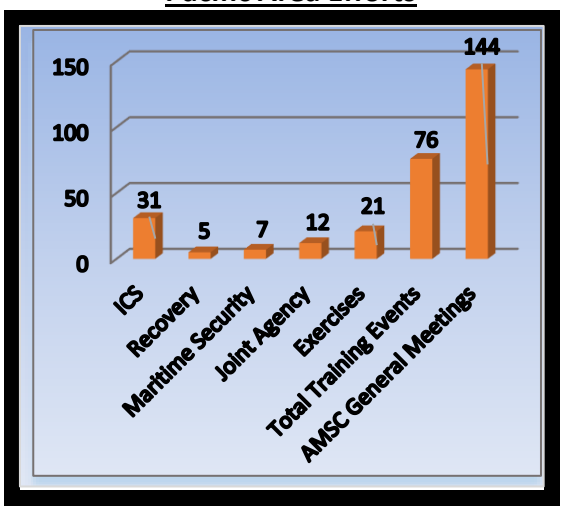


Figure 1 - AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners/stakeholders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

Cyber: AMSCs continued to engage in multiple cybersecurity related activities through various subcommittees to include the 31 established cybersecurity subcommittees. The AMSC subcommittees assist in addressing cyber risk, information sharing, and ways to enhance preparedness/resilience of cyber-related incidents. The following are a sample of AMSC cyber activities. The Boston AMSC, in conjunction with Massachusetts Emergency Management Agency, obtained funding for cyber assessments within their port. Sector New York's Cyber Liaison Officer has formed relationships with cyber professionals across several industries, many of whom are members of the Port of New York/New Jersey and Port of Albany AMSC, and has acquired knowledge of industry best-practices on cyber resiliency and recovery. Southeast Florida AMSCs' Cybersecurity Subcommittee sponsored three 1 day DHS Cyber Resilience Training Workshops. The training workshops allowed DHS Cybersecurity Advisors (CSAs) to provide assistance to stakeholders on protecting and sustaining services critical to the mission of their organizations. Eastern Great Lakes AMSC successfully obtained and is currently presenting four community cybersecurity trainings for their region.

AS/AT: AMSCs are addressing AS/AT concerns through subcommittees, training, drills and exercises, and by addressing preparedness, mitigation strategies and responses to an active shooter incident in the maritime domain through developing Concept of Operation Annexes and other response plans. Recognizing the need for AS/AT training for crew members of passenger ferries, the Southeastern AMSC and Sector staff, worked with the Coast Guard Research and Development Center (RDC) to aid in the development of a project with DHS Science and Technology Division in designing a Ferry Boat Security Training course. The pilot course was presented to the project team and key stakeholders on October 11, 2018 and final

revisions were made by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) on December 12, 2018.

UAS/Unmanned Aerial Vehicle (UAV): Unauthorized UAS/UAV over the air space of MTSA regulated facilities, commercial vessels, and other critical infrastructure continues to be reported. The Northeast Gulf of Mexico facilitated AMSC meetings to educate members on the current federal and state regulations governing "drone" usage and what actions they may take. Northern New England's AMSC partnered with the FBI Weapons of Mass Destruction (WMD) Boston Office, the University of Maine at Augusta, the University of Vermont, and the Maine National Guard to present five workshops to port stakeholders on UAS capabilities and threats.

Preventive Radiological and Nuclear Detection (PRND): The Domestic Nuclear Detection Office (DNDO) continues to support AMSCs in developing CONOPs and standard operating procedures, training personnel, and deploying detection equipment in support of the AMSCs preventive RAD/NUC initiatives. PRND challenges inspired the Sault Region AMSC to establish a robust Radiological Detection Program in conjunction with the DNDO by leveraging support from their Counterterrorism Operations Support Team (CTOS). CTOS brought a mobile training course to St. Ignace, MI and provided training for their federal, state, and local partners in maritime RAD/NUC detection procedures. The Mid-South AMSC participated in "Isotope Crossroads", a radiological transportation security tabletop exercise sponsored by the Department of Energy's National Nuclear Security Administration Office of Radiological Security and the FBIs WMD Directorate and Nuclear and Radiological Countermeasures Unit. The exercise promoted joint situational awareness, team building, and problem resolution in a crisis situation dealing with a WMD security-incident scenario involving Category 1 and 2 radiological/nuclear materials in commercial transit.

Active Threat Response Initiatives: A Long Island Sound (LIS) AMSC member, Cross Sound Ferry, succeeded in obtaining funding from the PSGP to develop an active threat response training program and plan for their crews that includes basic tactical training. The training also provides custom made scenario training videos. The LIS AMSC held a maritime focused Active Threat Response Table Top Exercise for their port partners, resulting in additional grant proposals to mitigate risks of an AS/AT incident in their COTP zone. Two LIS AMSC executive committee members spearheaded the Connecticut Operation by Response Agencies (a coalition of AMSC entities) efforts to conduct coordinated Joint Inter-State Maritime Security operations to collaborate on Law Enforcement/Security surge presence at Ferry Terminals during high risk exposure periods.

AMSC Participation in Cybersecurity Activities: Cybersecurity preparedness, prevention and awareness activities continued to expand, evolve and build momentum within St. Louis AMSCs. Representatives from the AMSC participated in the National Strategic Research Institute sponsored National Maritime Integration Office Workshop that provided a snapshot of

cybersecurity challenges within the inland river infrastructure. The workshop focused on best practices and lessons learned with respect to developing cyber risk mitigation, management strategies, challenges and information-sharing capabilities. The exercise outlined significant challenges with the Captain of the Port's comparatively limited influence over public/private core processes across an 80-mile linear port system. AMSC leadership also participated in a U.S. Secret Service Electronic Crimes Task Force Cyber and Operational Resilience Tabletop Exercise resulting in open dialogue between public and private port partners and sharing of industry best practices regarding network intrusion responses.

Arctic Maritime Symposium and Exercise: The Western Alaska AMSC members participated in the Alaskan Command (ALCOM) hosted Arctic Maritime Symposium. The event drew upon the expertise of Flag Officers, senior military leaders, intelligence analysts, interagency operators, and Arctic maritime subject matter experts to address the strategic challenges associated with Arctic maritime operations, planning, and security. AMSC members also participated in US Northern Command's (NORTHCOM) premier Arctic exercise, Arctic Edge 2018. Arctic Edge 2018 integrated personnel and platforms from across Alaska, to include ground, air, maritime and cyber operations in a deliberate evolution to expand the ability to secure our Arctic approaches and vital interests in the region.

5.0 Best Practices

AMSC reports identified many helpful and useful best practices. Below are highlights of specific programs, concepts and initiatives. Enclosure (4) identifies best practices reported from each AMSC in 2018.

Cybersecurity Information Sharing. The LIS AMSC executive coordinator distributes the weekly "Cyber Domain Situational Awareness" slide produced by the USCG Cyber Command to all AMSC and subcommittee port partners. This is shared with the Connecticut Cybersecurity committee and all regional maritime partners throughout the LIS COTP zone. Widest dissemination is emphasized.

Intelligence Subcommittee Partnerships. The Maryland - National Capital Region (NCR) AMSC intelligence subcommittee established participation from regional law enforcement and intelligence community partners. Their participation greatly improved information sharing and coordination on intelligence trends and analysis. This stakeholder partnership provides a maritime suspicious activity reporting mechanism for AMSC members, and advances a monthly multi-mission Intelligence Bulletin on specific maritime threats and emerging trends throughout the region. The AMSC INTEL subcommittee assisted with preparation for two real world events; the State of the Union Address and the Democratic Issues Conference.

Harmonization with Dispatch Agencies. The St. Louis AMSC conducted a Dispatcher Workshop involving six major regional jurisdictions from two states. Topics discussed were Intelligence

and Information Sharing, Operational Communications, resource requests, mutual aid protocols and existence of any Memorandums of Understanding (MOUs). AMSC participants navigated through regionally specific Complex Coordinated Terrorist Attack (CCTA) scenarios, focusing on a full spectrum of their port's Critical Infrastructure components, passenger vessels and MTSA-regulated facilities. Regional AMSC Subcommittees (i.e., Kansas City and Quad Cities AMSCs) also developed and conducted Dispatcher Workshops. As a result of the workshops, dispatchers gained an understanding of their positional authorities and importance of their roles in operational communication and coordination during a response to an incident in the maritime domain. The workshops also enabled managers and shift supervisors to understand and improve upon systematic vulnerabilities that existed in their initial incident response protocols.

UAS. To meet the growing demand for information in the area of UAS, the Houston Galveston AMSC created a UAS/DRONE subcommittee comprised of industry, law enforcement, first responders and port authorities. The goals of the subcommittee are twofold: first to educate and assist AMSC partners with the myriad of legal and procedural requirements to successfully start an organic UAS program and secondly to educate and assist partners with the rapidly growing topic of Counter Drone Technologies and legal issues.

Active Shooter Education and Training. Influenced by the 2017 mass casualty sniper shooting in Las Vegas, the Central California AMSC in 2018 embarked on educating Facility Security Officers (FSOs) at container terminals about methods to harden their truck gate access and deny access to container crane elevators and stairwells. This effort was designed to reduce the opportunity for a determined individual to access container cranes and fire down upon mass gatherings below. Additionally, Saint Mary's Medical Center in Long Beach has reserved the majority of their top floor as a site where counter-active shooter training can take place using non-lethal training ammunition.

AMSC Committee Meetings. Puget Sound AMSC conducts the general committee meetings in different locations of Sector Puget Sound's area of responsibility (AOR). Puget Sound ports are spread over a large geographical area. Inviting and encouraging the different ports to host the AMSC General Committee meetings has resulted in additional and more diverse attendance, better regional familiarity, and improved collaboration. The Executive Committee (EC) has started to co-locate their meetings with the Port Readiness Committee (PRC) meetings. Efficiencies are gained due to the significant overlap of membership.

Transportation Security Incident (TSI) Drills. The Southeastern New England (SENE) AMSC had identified a need to improve in the facilitation of AMSC Alert and Warning System (AWS) Notification drills. In 2018, The SENE AMSC successfully developed AWS protocols to alert members of the AMSC as well as Vessel Security Officers (VSO) and Company Security Officers (CSO) of a MARSEC level increase or other significant maritime security notification. The initial alert provided the staff with the mechanism to provide a short, but detailed, message

concerning a particular event and where to potentially receive more detailed information (such as Homeport 2.0, conference call, etc.). The alert also allows them to gauge the amount of confirmed received messages and provides a way for the staff to follow up with those that did not confirm receipt. Future notification drills are planned throughout the year and in conjunction with annual AMSTEP exercises.

6.0 Headquarters Input

This section provides insight into initiatives or amplifying information on specific topics typically discussed by AMSCs.

Cyber. CG-FAC continues to be at the forefront of developing guidance and other resources to address cyber safety, security, and cyber risk management within the MTS. The continually increasing role of cyber systems and the need to ensure the safety and security of ever-evolving technology and systems, for both information technology and operational technology, in the MTS was a strategic priority of FAC's work this past year.

Our office continued efforts to develop the draft Cyber Navigation and Vessel Inspection Circular (NVIC) that was released via the Federal Register in July of 2017. CG-FAC worked closely with Coast Guard legal offices to adjudicate over 200 comments, ensuring the best possible tool for the maritime community. The intent of the Cyber NVIC is to call industry's attention to MTSA regulations that require "radio and telecommunication systems, including computer systems and networks" to be addressed in facility security assessments. While the draft Cyber NVIC is going through review, units are encouraged to engage in conversations with facility owners, operators, and security officers about facilities' cybersecurity/cyber risk management programs and how to begin incorporating cyber into FSAs and FSPs.

CG-FAC also continued efforts to increase cybersecurity/cyber risk management awareness in the MTS through a cyber awareness webinar, developed in conjunction with ABS Group. This training, though meant for the Area Maritime Security Committees, was recommended to all members of the maritime community, including Coast Guard members. The webinar provides a "101" level awareness of cybersecurity/cyber risk management, terminology, systems, etc. that participants might encounter in their day-to-day work in the MTS and is available for the maritime community on the Coast Guard's *Maritime Commons* blog.

Our office emphasized the importance of incident reporting and information sharing throughout the MTS as being critical to cyber risk management efforts. Developing an MTS Cyber Incident Quick Response Card (QRC), which was distributed to Areas/Districts/Sectors for use in Command Centers. Additionally, we provided significant input into the National Command Center's QRC. These efforts improved alignment between the various QRC's and highlighted the areas of importance when reporting and responding to a cyber incident.

UAS. Coast Guard Headquarters, AMSCs, and the Federal Aviation Administration (FAA) are working on solutions to reduce the threat of increasing use of UASs, specifically unauthorized flights that could impact the MTS. The AMSC in New Orleans and Baton Rouge, developed a

method which reduced the number of reported erroneous unauthorized UAS flights by tracking authorized ones. The reporting network developed by their AMSC subcommittee has proven reliable. Segments of CG-FAC are working with the Coast Guard Operations Systems Center (OSC) to develop a voluntary "Notice of UAS Operations" submissions tool on Homeport. The objective is to develop a communications network similar to the one developed by New Orleans AMSC subcommittee. CG-FAC is also working on a policy letter to provide updated guidance on the procedure for reporting unauthorized UAS flights, which will align with the 2018 FAA Reauthorization Act reporting guidelines. There is currently a USCG UAS Community CG-Portal page that can be accessed by AMSC Executive Secretaries for collaboration on UAS related activities and policy developments.

A plethora of CG-HQ Program Offices, including CG-FAC, are participating in a number of DHS working groups to further address UAS concerns (e.g., Counter UAS External Engagement Working Group). A recent fact sheet on "Counter Unmanned Aircraft Systems Legal Authorities" was a product of the collaboration within these working groups.

NVIC 09-02, Change 5. CG-FAC worked to update the Navigation and Vessel Inspection Circular 09-02, change 5, "Guidelines for the Area Maritime Security Committees (AMSC) and Area Maritime Security Plans (AMSP) for U.S. Ports".

The updated NVIC provides guidance to Coast Guard COTPs, AMSCs, and the maritime community with the development and maintenance of AMS Assessments, AMSPs, and promotes unity of effort among all stakeholders with maritime security interests at the port level. One of the major revisions is enclosure 5 that now provides a Cyber Incident Response template that aligns with DHS's National Cyber Incident Response Plan.

AS/AT. CG-FAC collaborated with other program offices at Maritime AS/AT Implementation Planning Team (IPT) meetings in 2018. The focus was on identifying and addressing potential capability gaps in response to AS/AT events. A policy from the CG-MSR office (MSRO Policy Letter 03-18) states AMSCs members could assist the FMSC in developing capability and capacity by forging partnerships through AMSC meetings. Many AMSCs reported forming AMSC AS/AT subcommittees, conducting active shooter drills and exercises, implementing Active Threat Response Plans, and developing training programs for crew members on passenger ferries in 2018.

MTS Resilience/Recovery. The 2018 Hurricane season was busy affecting Guam, the Northern Mariana Islands, Hawaii, North and South Carolina, and the Alabama/Florida Coast and required ports to prepare for and respond to a MTS disruption. National planning for these hurricanes included identifying Coast Guard PSSs and Security Specialists (Port/Recovery) from outside the impacted areas to prepare for deployment in support of MTS Recovery operations at affected units and coordinating with Customs and Border Protection and Department of Transportation personnel managing the FEMA Emergency Support Function One response. This was particularly important in locations that don't have a SS (P/R) specialist. MTS Recovery Units at the Area, District, and Sector level which included participation from other Federal, Territorial,

Tribal, State, Local, Private and Public port stake holders were integral to effective short-term recovery and resumption of commercial maritime operations to those impacted areas.

In 2018, NVIC 04-18, the Template for the Marine Transportation System Recovery Plan (MTSRP), was released creating a MTSRP for each COTP zone. This plan should be referenced within Section 6000 of the AMSP. This was a major accomplishment and makes the MTSRP an All Hazard plan instead of merely responding to a TSI.

7.0 Conclusion

Through collaboration, planning, coordination, open lines of communication, and unity of efforts, AMSCs have proven to be and remain essential to addressing new issues and emerging threats that could impact our national security and economic interests. AMSCs still have a role in identifying, analyzing, prioritizing, and mitigating both physical and cyber related challenges in the MTS to advert potential adverse impacts to critical waterways and ensure efficient facilitation of commerce.