Area Maritime Security Committee

Challenges, Suggestions, Accomplishments, and Best Practices

2019 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 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 whom advice the COTP/FMSC on mitigation strategies to ensure the safety, security, and resiliency of our nation's critical MTS.

The 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. The report assists CG-FAC in devising national strategies to address common problems, emerging threats, validate port specific data, track AMSC activities nationwide, and measure AMSCs alignment with national preparedness goals. The report provides the opportunity to review and discuss the implications of the consolidated report with other program offices in regards to their policies and procedures that impact the MTS.

Bradley W Clare

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

1.0 Background

The AMSCs were mandated by the MTSA of 2002 to provide a link for contingency planning, development, review, and updates to the Area Maritime Security Plans (AMSPs), and to enhance communication between port stakeholders within federal, state, local, tribal, and territorial government and private sector stakeholders to address maritime security issues. In 2019, each AMSC assisted with the five year review, assessment, and incorporation of changes to their respective plans. This year-long update process involved substantial effort by both Captain of the Port staff and members of their respective AMSCs. FMSCs and their AMSCs tested the effectiveness of their updated port-level AMS Plans and supported maritime security preparedness regimes through the engagement of their port stakeholders. AMSCs continue to be a vital partner in securing the MTS.

2.0 Challenges

AMSCs identified specific challenges or impediments encountered in 2019. Enclosure (1) identifies all challenges reported from each AMSC in 2019. The following entries highlight common challenges:

Cybersecurity and the MTS. Cybersecurity was identified in the AMSC annual reports as a reoccurring challenge. AMSCs are often unclear on their roles and responsibilities in regards to port wide cybersecurity. The technical aspects may present constraints to personnel with limited knowledge of Information Technology (IT) systems and cyber technology. Vessel and facility security officers for example often rely on their IT personnel and their legal departments when reporting potential or actual cybersecurity incidents. Even though some AMSCs performed extensive efforts to promote cybersecurity awareness and preparedness with the public and port partners, there remain gaps in the efforts to reduce maritime cyber vulnerabilities.

Unmanned Aircraft Systems (UAS) access to the MTS. Independently, port and maritime industry partners have worked together to capture and report the increase in UAS activity flying over vessels and facilities, quantifiably identifying UAS as a serious emerging threat to maritime safety and security. Public drone usages continues to be a planning challenge during security events for some AMSCs. Port stakeholders have been questioning what enforcement options are in place for UAS incursions on their facilities. Current guidance does not sufficiently address security risks associated with unauthorized operation of UAS' in restricted areas.

Homeport 2.0. Homeport is the United States Coast Guard's enterprise Internet portal for the Maritime Community. It was designed initially to support the secure information sharing between Coast Guard personnel, members of the maritime community, and designated port stakeholders as per MTSA. Since this application's update to the 2.0 version, many port stakeholders have ceased using Homeport and have chosen other platforms to share information such as HSIN, Adobe Connect or email distribution lists. Many are reporting that error messages and system downtime are becoming increasingly common. For example, during one AMSCs 2019 Full Scale Communications Exercise, the self-service password reset function failed frequently and many stakeholders were unable to change their MARSEL Level during the exercise which required the Homeport Manager to track attainment manually via a spreadsheet.

Port Security Specialist (PSS) Training. The PSS' predominately serve as the AMSC executive secretaries. Many of the responsibilities of the PSS require continual training to perform their duties. These duties are diverse and the training and policy updates of these duties come from several different directorates (e.g., CG-FAC, CG-PSA-2, CG-MSR, etc.). Annual CG-C-School training specifically for the PSS' remains lacking.

Interoperable Communications. Interoperable communications with local and state agencies continues to be an issue for some AMSCs. Many rely on cellular telephones, which are vulnerable to disruptions and outages during real world events. Another AMSC uses a specific system for maritime communications but not all stakeholders have this system installed. There is a need to establish and maintain common communication avenues between the multiple response agencies.

Active Shooter (AS)/Active Threat (AT). Response readiness to AS/AT scenarios in the maritime domain is extremely limited by availability of assets, inconsistent security protocols on public access vessels and lack of coordinated response protocols among federal, state, and local authorities. Available training for local law enforcement appears to be primarily focused on land based incidents and do not adequately address the unique challenges of response aboard an underway vessel such as a passenger ferry. Recommendations included additional policy guidance and training.

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 2019:

Cybersecurity/Cyber Risk Management. AMSCs continue to suggest the need for more definitive guidance on cybersecurity that addresses the MTS. Training was a reoccurring gap identified in the reports. Some suggested providing specific training for their stakeholders. Additionally, training Coast Guard personnel so they can address stakeholders' concerns, which would subsequently increase awareness and continuity nationwide. Another suggestion was to provide assistance in planning for cyber security exercises.

Homeport 2.0. The PSS' are the executive secretaries of the AMS Committees and according to the reports still do not have the tools necessary to manage Homeport external stakeholder end users in a fashion similar to what was available in Legacy Homeport. AMSCs reports continue to suggest the restoration of tools needed for effective management of Homeport.

UAS. AMSCs are advocating for an update to 18 United States Code (USC) to include legislative language to implement UAS countermeasures. Furthermore, some are suggesting a need for UAS guidance for MTSA regulated Facility Security Plans (FSPs) and Vessel Security Plans (VSPs). Training on UAS detection and deterrence (countermeasures) was also a focal point provided by the AMSCs.

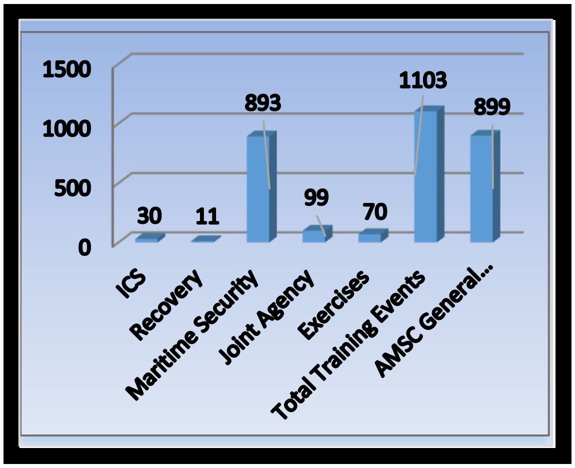
Active Shooter (AS)/Active Threat (AT) Incidents: One AMSC summed up the main suggestions that would be applicable to all. Continue to evolve and expand the Coast Guards' maritime AS/AT policy, training, tactics and procedures. Further assess any potential changes to facility and vessel security protocols under the MTSA that might assist vessel and facility operators in implementing best-practices to guard against and respond to an AS/AT attack.

Interoperable Communications: Delaware Bay AMSC submitted a very detailed suggestion on how to improve Maritime Domain Awareness (MDA) and reduce response risks. An investment in a nationwide network that creates interoperable communities capable of ad-hoc, on demand sharing of video, radio, text, voice, data, and telephone communications real-time and in a secure environment continues to be needed. They suggested a network similar to New Jersey's Mutualink system be implemented nationwide.

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 2019, AMSCs and their respective subcommittees collectively facilitated 2,189 events. This total included 1,010 administrative AMSC meetings (e.g., Executive Steering Committees and General AMSC meetings) and 1,179 training specific events (includes 108 joint agency training meetings, 927 maritime security training operations, 97 training exercises, 33 Incident Command System training sessions and 14 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.

Atlantic Area Efforts



Pacific Area Efforts

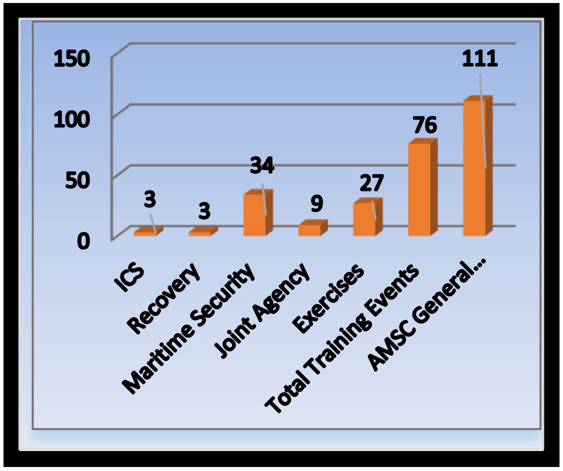


Figure 1 - AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners and 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: Cyber continues to be a key area of focus for AMSCs. AMSC cybersecurity and intelligence subcommittees sponsored an increasing number of cyber training seminars and workshops, and promoted exchange of government and industry best practices focused on identification of vulnerabilities and risk reduction within the MTS. The following are examples of AMSCs activities and efforts. The Port of New York/New Jersey and Port of Albany AMSC assisted in the presentation of a series of Cybersecurity Table Top Exercises (TTXs). Additionally subject matter experts were invited to a workshop to assist CG Headquarters in the development of the Maritime Cyber Security Risk Assessment Model (MCRAM). Southeast Alaska AMSC cyber subcommittee partnered with Sector Juneau Intel in the development of a regular cyber communication forum to ensure partner awareness of relevant maritime cybersecurity issues. The Sabine Neches AMSC was invited to participate with the Port Readiness Committee in a joint U.S. Transportation Command, USCG, and Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity exercise to address challenges specific to Strategic Ports of Embarkation. CISA's Industrial Control Systems Joint Working Group engaged with members from the Kansas City AMSC (Regional to Saint Louis AMSC). The workshop sessions helped bridge the awareness gap as the AMSC and Sector developed Cyber Incident Response Plans.

AS/AT: Potential AS/AT incidents in the maritime environment received significant attention by AMSCs in the planning, training and exercising of coordinated responses in 2019. Southeast Alaska AMSC's Law Enforcement (LE) subcommittee helped to establish an AS/AT local training alternative by utilizing a local FLETC Certified Trainer and a dormant processing plant. The Puget Sound AMSC planned and executed an innovative and comprehensive policy rollout and associated exercise series that markedly boosted regional active threat preparedness. New Orleans AMSC LE subcommittee sponsored a Full Scale (FS) Active Shooter Exercise at two locations in the port resulting in improved preparedness and future collaborate training and exercise efforts. Leveraging the robust LE network of the Neptune Coalition, the Northern California AMSC developed a Maritime Active Threat Response Plan designed to provide a swift and coordinated response to an AS/AT on Soft Targets and Crowded Places. The response plan synchronizes Coast Guard and partner Tactics, Techniques, and Procedures, equipment, training levels, and waterborne assets among partners, and will be added as an annex to their AMSP.

UAS/Unmanned Aerial Vehicle (UAV): Unauthorized UAS/UAV over the air space of MTSA regulated facilities, commercial vessels, and other critical infrastructure continued to be reported in 2019. A number of AMSCs chartered working groups and subcommittees on UAS concerns. The Gulf of Mexico (GOM) AMSC established a UAS working group to address the potential impact of UAS usage offshore and the lack of current UAS regulations or guidance developed for offshore UAS usage. Northern California AMSC chartered an UAS workgroup in response to their region's increased presence of UAS, and lack of consistent approach to responding to potentially unsafe UAS activity. The Houston-Galveston AMSC created a UAS subcommittee and their charter focuses on sharing information on new technology, identifying best practices, reviewing counter UAS technology and policies, and disseminating new state and federal UAS regulations to port stakeholders.

Preventive Radiological and Nuclear Detection (PRND): The Sault Region AMSC encountered its first real-world maritime PRND event in 2019 during the Mackinac Bridge Walk in the form of a positive detection while enforcing a safety zone. This was particularly important because the AMSC members had worked over the past five years to bolster its primary and secondary PRND capabilities through the Port Security Grant Program (PSGP), former Domestic and Nuclear Detection Office (DNDO) grants, and other means. The Mackinac Bridge Walk in the Straits of Mackinac is the largest event in their COTP zone, with tens of thousands of people participating annually. The successful evolution proved that detection was possible, the plan was successfully followed, and the training and equipment provided a capability that improved the safety of their maritime events.

Maritime Domain Awareness: Sector New York, NY/NJ AMSC, and the New York City Police Department (NYPD) share the goal of enhancing maritime security in and around the Port of New York/New Jersey. The NYPD routinely conducts flights in the Sector New York COTP Area of Responsibility (AOR) for law enforcement purposes. The NYPD aviation assets are equipped with cameras funded from the PSGP. The cameras provide real time video feeds and still imagery to the NYPD operations center. The MOU between the USCG and NYPD set forth the terms by which the NYPD will conduct flights to assist the USGG and provide the USCG with access to aviation video feeds, as well as still imagery, in order to enhance both agencies abilities to monitor inbound vessel traffic, ports, waterways, and facilities within the Sector New York AOR.

AMSC Participation in Updating the AMSP: AMSCs were instrumental in completing the 5-year revision and formal re-approval of their AMSPs. This complex and time-consuming effort was one of the most significant accomplishments of 2019. Some AMSCs used the new template provided in NVIC 09-02 (series) to establish an AMSC cyber response annex to their AMSP. Each AMSC conducted an Area Maritime Security (AMS) Assessment to review the threat landscape in individual AORs. For example, the Western Florida AMSC conducted an assessment by a working group, which included AMSC members, to review any significant security issues or changes noted since the last formal assessment. If significant changes were noted then it is possible that the top three Transportation Security Incident (TSI) scenarios would need to be updated and the changes to the plan subsequently validated through the Area Maritime Training and Exercise Program (AMSTEP) process.

Western Alaska AMSC 2019 Exercises: Member agencies, Sector Juneau, Sector Anchorage, District 17, and AMSC subcommittees participated in the Centers for Disease Control (CDC) sponsored TTX simulating an infectious disease arriving in Alaska via a cruise ship. Member agencies and all AMSC regional subcommittees also participated in the statewide Alaska Shield Full Scale Exercise (FSE). AMSC members participated in the design, development, and execution of Arctic Expeditionary Capabilities Exercise, the first amphibious assault exercise to take place in Alaska since 1987.

Risk Reduction, and Resource Assessment Model (3RAM): The U.S. Coast Guard, select Puget Sound AMSC members, Washington State Ferries and Washington State Patrol (WSP) have been engaged in the creation of 3RAM. 3RAM is a flexible, quantitative risk assessment tool that surpasses vehicle-borne improvised explosive devices screening requirements outlined in MARSEC Directives 104-5 and 105-2, by effectively assigning resources to mitigate risk. This revised deployment better uses existing WSP staff to deter and react to active threats within the ferry system. The pilot deployment program is in process and continues to collect data and refine the deployment strategy.

Active Shooter Quick Response Card: The Delaware Bay AMSC Maritime Tactical Operations Working Group (MTOG) sponsored a four-hour seminar bringing together the various LE agencies in the COTP zone that would be responsible for notification, protection, prevention, response to and recovery from an active shooter incident in the maritime environment. The main emphasis of the seminar were active shooter planning considerations and development of an active shooter Quick Response Card (QRC). The information compiled will be used in an annex to the AMSP as a Concept of Operations (CONOPS) Active Threat Response Plan.

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 2019.

Cybersecurity Information Sharing. The majority of the AMSCs have established cyber subcommittees to address cyber security risks. The subcommittees have proven to be an excellent forum for identifying cyber vulnerabilities, risk reduction and resiliency efforts, establishing reporting requirements for cyber-incidents, and determining protocols for response and mitigation efforts. AMSC Long Island Sound Executive Secretary distributes the weekly "Cyber Domain Situational Awareness" slide produced by USCG Cyber Command to all AMSC and subcommittee and all regional maritime partners throughout their COTP zone. The Delaware Bay AMSC Cybersecurity Subcommittee created a one-page Cyber Guide brochure that outlines the reporting processes as well as providing countermeasure tips, and federal, state, and local resources for port stakeholders. Ohio Valley AMSCs continue to promote cybersecurity awareness for members by publishing cybersecurity information on HOMEPORT, conducting cybersecurity workshops, and promoting attendance at regionally held US DHS sponsored cybersecurity training sessions. Northern California AMSC also continues to publish a quarterly Cybersecurity Newsletter.

Senior Leader Workshops. The St. Louis AMSC along with its regional AMSC subcommittees developed and conducted Senior Leader Workshops for law enforcement and fire department field supervisor agencies. The workshops provided 193 participants from 104 agencies Sector-wide to navigate through regionally specific Complex Coordinated Terrorist Attacks (CCTA) scenarios, utilizing Master Scenario Event List scenario attack events, focusing on maritime Critical Infrastructure, key commercial assets (Soft Targets – Crowded Places), passenger vessels, and MTSA-regulated facilities. These PSS facilitated workshops provided exceptional value for local AMSC members by highlighting the importance of maintaining regional awareness and the potential need for non-organic response resources.

Maritime Domain Awareness (MDA). The LA/LB Regional Coordinating Mechanism (RECOM) working with a vast array of port partners, including key members of the Central California AMSC, are promoting interagency collaboration in the maritime community. Members worked together to disrupt transnational criminal organizations and maximized the use of all available resources which improved interagency relationships. These efforts significantly extended the operational reach of each organization, bridged communication and coordination gaps, and improved MDA. The sharing and use of tactical data among multiple agencies supported successful operations, increased operational tools for all agencies and created a successful blueprint for interagency mission coordination and execution.

UAS. Eastern Great Lakes AMSC established protocol to respond to UAS Operators during a maritime event. During the 2019 Tall Ships event, there were two separate reports of UAS' operating within the event footprint. The protocol consisted of contacting the Incident Command Post (ICP), locate the Operator (if possible), send law enforcement that were already on site to contact and tell the operators to cease UAS operations, and investigate as needed. The two operators of the UAS were identified and both grounded. Sector New York utilized UAS devices to provide surveillance support to AMSC LE partners during the NYC Marathon, further strengthening the already well-established working relationship.

Active Shooter Education and Training. The Port of New York/New Jersey AMSC established a Small Passenger Vessel Committee to address AS/AT Response. In conjunction with this effort an AS/AT Concept of Operations Plan was developed with the assistance of multiple AMSC LE and OGA stakeholders. Other COTP/AMSC initiatives included a one day seminar on how individuals without medical training can assist victims from an AS/AT event. Numerous ferry crew members from a variety of NYC companies attended the seminar. Southeast Alaska AMSC partnered with Petersburg Police to address AS/AT training. In 2019, Ohio Valley AMSCs conducted active shooter and underway boat drills providing an opportunity for law enforcement agencies to practice response to an active shooter threat occurring in the maritime domain, and training for commercial passenger vessel crewmembers on an active shooter threat. In response to CGHQ and D13 prioritization of AS/AT challenges, Puget Sound AMSC jointly developed a new Maritime Active Threat Plan (MAT-P) that supports coordinated active threat response, and equip LE, passenger ferry and industry partners to prepare for and respond to an active threat.

AMSC Committee Meetings. Columbia River AMSC Executive Secretary and members have made every effort to minimize the time and cost incurred by their industry partners to attend meetings at Coast Guard locations. The AMSC has continued the practice of hosting both an "Industry Breakfast" and a Quarterly AMSC Meeting at MSU Portland on the same day and location. Although the agendas are different, there is considerable overlap in attendees, which minimizes their travel time. A teleconference line and remote access to slides and other briefing materials has improved attendance by geographically remote members. The Columbia River AMSC will continue these practices and recommends consideration by other AMSCs.

TSA I-STEP Exercise. Sector Southeastern New England (SENE) staff and various SENE AMSC members participated in TSA's Intermodal Security Training and Exercise Program (I-STEP) one day exercise in 2019. Participation included federal transportation security and preparedness partners, state transportation and emergency management authorities, local law enforcement, and multimodal transportation organizations from the Providence, RI-area. The exercise consisted of three interactive tabletop modules preceded by briefings from TSA's Intelligence and Analysis (I&A) and the Department of Homeland Security's (DHS) Countering Weapons of Mass Destruction (CWMD) Office. Discussions addressed the prevention, protection, mitigation, response, and recovery activities from an intermodal security incident to include an active shooter event. Encourage participation, if provided the opportunity, to assist in the planning of a TSA I-STEP exercise to support the intermodal maritime segment.

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 oversaw the successful publication of Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities. This NVIC provides guidance to facility owners and operators on complying with the requirements to assess, document, and address computer system and network vulnerabilities. This NVIC is intended to assist regulated facility owners and operators in updating Facility Security Plans (FSPs) and Alternative Security Plans (ASPs) to comply with existing MTSA regulations. It is intended to assist in identifying computer systems and network vulnerabilities which could cause or contribute to a TSI, Breach of Security (BOS), and/or the identification of Suspicious Activity (SA). An implementation period will allow time for facility owners and operators to review their computer systems and networks and update their Facility Security Assessments (FSAs) and FSPs.

To support the Facility Cyber NVIC, CG-FAC released and maintains a Frequently Asked Questions document to address questions as maritime industry and Coast Guard field commands review the NVIC. Additionally, our office released a Facility Inspector Job Aid in order to provide marine safety personnel with additional guidance as they address facilities' documented cyber vulnerabilities. This publication provides the workforce with another tool needed to ensure compliance with regulatory requirements.

CG-FAC also continued efforts to increase cybersecurity/cyber risk management awareness in the MTS through training, guidance, and awareness. In addition to continuing to emphasize the cyber awareness webinar, developed in conjunction with ABS Group, we continue to work with other programs to identify opportunities to enhance cyber knowledge throughout the service. Program offices at Headquarters are working together to develop cyber training for the field, recognizing that training and education will continue to evolve as the workforce becomes increasingly cyber-aware, while also acknowledging the ever-changing cyber landscape.

In response to Congressional direction in the FAA Authorization Act of 2018, CG-FAC continued to lead efforts towards development of a Maritime Cyber Risk Assessment Model. This model will allow for users to conduct baseline cyber risk assessments for a facility or port and is being developed for use by maritime stakeholders ranging from port authorities and Area Maritime Security Committees (and Cybersecurity Subcommittees) down to individual facility owners/operators/security officers. Developed in coordination with the MITRE Organization, this voluntary model will incorporate the aspects of NVIC 01-20 as well as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and will be customizable based on the needs/focus of the specific user. As we reach the completion of this initial model, CG-FAC will conduct outreach with maritime industry while also reviewing ways to build upon this initial model.

UAS. Coast Guard Headquarter Program Offices continue to participate in DHS UAS working groups to implement the guidelines from the 2018 Federal Aviation Administration (FAA) Reauthorization Act. FAA published a guidance memorandum in 2019 for authorized federal Counter-UAS users (who are required to coordinate with FAA). The Coast Guard subsequently provided specific requirements in an internal Policy Letter on operating/deploying C-UAS for authorized units. Other Headquarter initiatives include the CG-MSR office facilitating the Strategic Guidance Team (SGT) and Working Group (WG) that supports DHS's C-UAS Pilot Program. CG-FAC is working on MISLE enhancements for BOS/SA reporting to assist with tracking the UAS threat in the MTS.

The USCG UAS Community CG-Portal page (internal) continues to provide resources and latest developments. The FAA website can be accessed by the public and provide additional resources. For example, the Public Safety Small Drone Playbook provides a plethora of information for public safety officials and can assist in determining the difference between authorized and non-authorized drone operations.

NVIC 09-02, Change 5. This NVIC, "Guidelines for the Area Maritime Security Committees (AMSC) and Area Maritime Security Plans (AMSP) for U.S. Ports." was signed by the Assistant Commandant for Prevention Policy on April 19, 2019. The updated NVIC provided guidance to Coast Guard operational commanders, AMSC members, and the maritime community with the development and maintenance of Area Maritime Security (AMS) Assessments, AMSPs, and promotes unity of effort among all stakeholders with maritime security interests at the port level. In addition, the NVIC provided a template to ensure AMSP consistency nationwide, but allowing for flexibility due to different variables port to port.

AS/AT. CG-MSR developed the pilot Advanced Law Enforcement Rapid Response Training (ALERRT) Maritime AS/AT Course. CG-MSR with support from the Office of Law Enforcement Policy, and DCMS-34 hosted two one-week pilot AS/AT Train the Trainer Courses for 45 Coast Guard Members from 27 different units in 2019. The purpose was to improve regional response capabilities in engaging AS/AT in the Maritime Domain and standardize tactical procedures. AMSCs continued in 2019 to work with port stakeholders and LE subcommittees to plan, train, and conduct exercises in response to a potential AS/AT maritime event.

MTS Resilience/Recovery. The 2019 Hurricane season was busy with four named storms affecting the US east and gulf coasts. Multiple ports were required to prepare for and respond to an MTS disruption. National planning for these hurricanes included identifying Coast Guard PSS and Security Specialists (SS)/Port/Recovery (P/R) from outside the probable 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 do not 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 stakeholders were integral to effective short-term recovery and resumption of commercial maritime operations to those impacted areas.

In 2019, COMDTINST 16000.28B Marine Transportation System Recovery Policy and Operations was signed. This policy requires all COTPs to have a stand-alone recovery plan (Guidelines located in NVIC 04-18). All COTPs have written and received approval for these plans.

7.0 Conclusion

AMSCs have a role in assisting and advising the COTP/FMSC on current and emerging challenges in the MTS that could adversely impact the Maritime Domain within their COTP Zone. Through fostering collaboration, the sharing of ideas and information, and the regular engagement with the COTP/FMSC and staff, the AMSCs have proven themselves as valuable assets within the maritime security regime.