Area Maritime Security Committee

Challenges, Suggestions, Accomplishments, and Best Practices

2020 Annual Report

U.S. Coast Guard

Washington, D.C.

Table of Contents

Online Enclosures (Internal access only)

Enclosure (1) Challenges as reported by the AMSCs

Enclosure (2) Suggestions as reported by the AMSCs

Enclosure (3) Accomplishments as reported by the AMSCs

Enclosure (4) Best Practices as reported by the AMSCs

Office of Port and Facility Compliance (CG-FAC)

Office Chief's Perspective

Area Maritime Security Committees (AMSCs) are an incredibly valuable focal point for regional collaboration to enhance maritime security at the port level. They 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), and they succeed based on the strong participation from government partners and industry stakeholders.

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 approximately 31 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 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, bolstering the safety and security of the MTS.

AMSC annual reports are an important tool for sharing information between AMSCs and assisting with national strategies to address common issues and emerging threats. This Annual Report highlights the many achievements of the AMSCs across the country and serves as a reminder of all the outstanding work performed in 2020 to secure the MTS in the face of unprecedented challenges.

Andrew J. Meyers,
Captain, United States Coast Guard
Chief, Office of Port and Facility Compliance

1.0 Background

AMSCs were mandated by the Maritime Transportation Security Act (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 and all levels of government. Local AMSC annual reports are an important tool used to compile and share information pertaining on 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. They ultimately serve to improve AMSC effectiveness nationwide. AMSCs continue to be a vital partner in securing the MTS.

2.0 Challenges

AMSCs identified specific challenges or impediments encountered in 2020. Enclosure (1) identifies all challenges reported from each AMSC in 2020. The following entries highlight common challenges:

Impacts of COVID-19. Communication and information sharing is key to AMSC success. In most cases, AMSCs held virtual meetings throughout the year due to Center for Disease Control and Prevention (CDC) guidance during the global pandemic. Conducting effective AMSC outreach and coordination with port partners presented significant challenges. Specifically, AMSC meetings held via virtual platforms presented security concerns when the need to pass sensitive information arises.

Cybersecurity and the MTS. The dynamic nature of cybersecurity threats make cybersecurity preparedness, response, and recovery a continuing challenge. There is a noticeable lack of cyber expertise among some AMSC's membership and regulated facility or vessel operators. A copious amount of information on cyber is being shared, but there is a gap in the technical expertise to translate this information into actionable efforts. National Response Center cyber-breach of security reports are distributed too broadly and include legacy environmental entities, which results in some reluctance in reporting. The future expectations in the cyber domain and how they will impact federally regulated MTSA facilities and other port stakeholders remains a concern to many AMSCs.

Unmanned Aircraft Systems (UAS) access to the MTS. UASs continue to pose a heightened security threat, and local industry and law enforcement partners are seeking prevention, response and mitigation solutions. AMSCs voiced a need for more enforcement options addressing unauthorized UAS flights related to vessels and facilities in the port region. The lack of federal policy, guidance, and enforcement has impacted how port stakeholders can mitigate this gap within restricted air spaces above maritime infrastructures. UAS encounters continue to generate questions and concerns.

Homeport 2.0. Homeport is the United States Coast Guard's enterprise internet portal for the Maritime Community. The current version, Homeport 2.0, functionality continues to be an issue for member account management and for communicating effectively with maritime stakeholders. It is nearly impossible for account management to occur at the field-level, making "buy-in" from AMSC members challenging. Error messages remain a common issue as users attempt to make progress in the system. Issues with the system were amplified due to the number of personnel who had to work remotely as per COVID-19 CDC guidance.

Maritime Security Risk Analysis Model (MSRAM). MSRAM is one of the tools used by the AMSCs in conducting the Area Maritime Security Assessments. The Risk Management Workspace tool in MSRAM needs to be updated to ensure the most current data is used for Risked Based Maritime Security and Response Operations activities. Completing MSRAM updates and verifications in 2020 was made extremely difficult due to the pandemic environment hindering field level verifications and systems were challenged when working remotely due to the size of MSRAM's digital footprint.

Emerging Challenges. "Unmanned mini self-propelled semi-submersible vessels" have been observed in some COTP zones that may require development of protocol for identification and analysis to ensure intent and purpose. Offshore windfarms are being developed, which will result in new and complex challenges associated with critical infrastructure protection of these assets.

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 2020:

Cybersecurity/Cyber Risk Management. AMSCs continue to highlight the need for more definitive guidance on cybersecurity that addresses the MTS. Some suggested to implement national policy that provides a standard approach or framework for sharing cyber Indicators of Compromise (IOCs) or Indicators of Attack (IOA) or both with public and private sector IT and Cybersecurity professionals external to the USCG who are in the best position to take protective measures within their organizations. Additionally, serious consideration should be given for inclusion of Cyber Transportation Security Incidents (TSIs) in AMSPs, even if not identified as one of the top three scenarios.

Homeport 2.0. Homeport 2.0 does not allow the AMSC Executive Secretaries to manage external stakeholder accounts (password resets, profile updates, etc.) as was available in Homeport 1.0. Moreover, the end user experience appears to be lacking. Suggest the setting up of the AMSC community's layout and functionality be similar to the PHP Bulletin Board[1] forum software.

UAS. A reoccurring suggestion states UAS guidance should be provided for MTSA regulated facilities, which can be adapted into their individual security plans. Some progress was noted in this area, but still no published guidance. Additionally, some AMSCs noted a growing interest from AMSC partners and MTSA facilities regarding the use of and regulatory constraints in the field of UAS Countermeasures. Most are aware of national DHS and FAA testing and use of UAS Countermeasures on high visibility, national events, yet the AMSC community would benefit from improved messaging and transparency regarding the future development of DHS and FAA policy and kinetic systems that are being tested and used for large scale events.

Active Shooter (AS)/Active Threat (AT) Incidents: An AMSC proposed developing a nationwide policy on using an audible AS/AT alarm at CG stations in ports that have a high volume of passenger ferries, tourist boats, and cruise ships, which would be distinctly different from a SAR Alarm. Another AMSC felt a greater level of clarity regarding best practices and standards for hardening MTSA-regulated entities against AS/AT is needed, along with additional guidance on implementing these standards into security plans.

Recovery and ICS for AMSC Members: A small-group virtual Incident Command System (ICS) training was suggested. The training audience would be AMSC port partners. The training would differ from the Federal Emergency Management Agency (FEMA) ICS training, and members would be able to access the training prior to an Area Maritime Security Training and Exercise Program (AMSTEP) scheduled exercise. Additionally, another AMSC proposed we should allow AMSC members to attend CG's ICS 300, ICS 339 and/or ICS 400 online training.

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 2020, AMSCs and their respective subcommittees collectively facilitated 1,843 events (many events made possible using virtual platforms). This total included 793 administrative AMSC meetings (e.g., Executive Steering Committees and General AMSC meetings) and 1,050 training specific events (includes 137 joint agency training meetings, 800 maritime security training operations, 82 training exercises, 28 Incident Command System training sessions, and 3 MTS Recovery Unit

[1] https://www.phpbb.com/about/

training sessions). These coordinated opportunities resulted in effective, real world security prevention, response, and recovery efforts. Enclosure (3) identifies accomplishments reported from each AMSC.

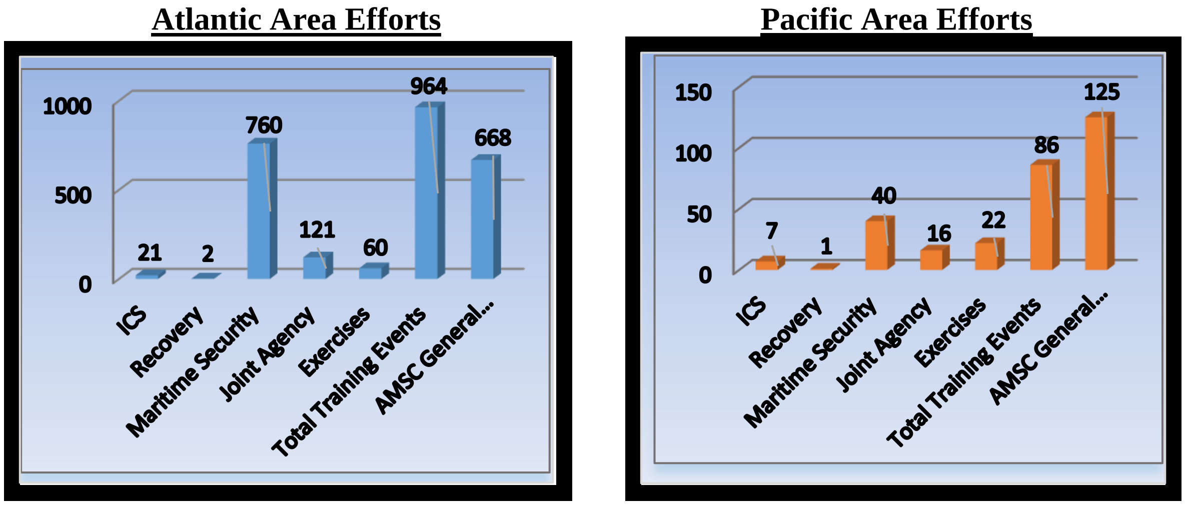

Figure 1 – AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners 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 from each AMSC.

Cyber: Cybersecurity remains a continuing theme for AMSC subcommittees. The Northeast Gulf of Mexico AMSC conducted Cyber Awareness training at several subcommittee meetings by various Subject Matter Experts (SMEs). The Port Security Specialists (PSSs) continue to engage stakeholders in cyber discussions and training as a part of the cyber awareness campaign. Outreach was also conducted to maintain linkage with the DHS National Cybersecurity and Communications Integration Center (NCCIC).

With the advent of maritime security management activities moving to a virtual domain, cybersecurity preparedness, prevention, and awareness activities became a priority discussion for the Saint Louis AMSC and its Regional Subcommittees. PSSs coordinated and developed cybersecurity awareness training and socialized the Cyber Incident Response Plan and a Cyber Incident Action Plan framework to support cyber-related events in their Area of Responsibility (AOR) as appropriate.

The Puget Sound AMSC planned and executed an innovative and comprehensive virtual cyber exercise. The AMSC members, along with efforts from CG Sector Puget Sound, combined their insights and teambuilding skills to craft an agenda that focused on educating maritime agency and industry stakeholders, and solicited and identified policy and implementation issues that industry would like addressed.

The Port Security Grant Program (PSGP) provided funds for a variety of cybersecurity projects. For example, the Hawaii and American Samoa AMSC received close to one million in funds to remediate cybersecurity risks identified at a major port critical infrastructure.

Resiliency: Sector Upper Mississippi River (UMR) port-wide communities' endured significant challenges in 2020. The eleven-state AOR saw significant events both natural and man-made. The PSS staff and AMSC partners responded to flooding, COVID-19, civil unrest, weapons related activities near MTSA-regulated facilities, and a myriad of other relevant issues. Sector UMR, along with public/private AMSC port partners, quickly responded and adapted to the realities of the rapid community spread COVID-19 virus. Maintaining operational sustainability of the MTS and protection of personnel and critical infrastructure remained the COTP focal priorities. Protocols were swiftly developed and swiftly deployed for all Sector UMR maritime security mission elements to include river industry operations and passenger vessel operations.

UAS/Unmanned Aerial Vehicle (UAV): Reports of unauthorized UAS/UAV over the air space of MTSA regulated facilities, commercial vessels, and other critical infrastructure spurred AMSCs to apply a variety of new measures/initiatives. The Port of New York and New Jersey AMSC coordinated with port partners to obtain Counter-UAS (C-UAS) support when USCG and Other Government Agency (OGA) resources were escorting vessels of interest transiting their COTP zone.

Northern California UAS workgroup provided facility operators with a UAS reporting framework using the Federal Aviation Administration's (FAA's) best practice handout to assist in recognizing UAS suspicious activities.

The Delaware Bay AMSC arranged a presentation on cutting edge UAS technology providing valuable insight on C-UAS capabilities, current laws and regulations, which subsequently provided the materials for the AMSC to develop a UAS brochure, now used extensively by the Facility Security Officer's in their AOR.

Radiological/Nuclear (RAD/NUC) AMSTEP: The Louisville and Southern Indiana Regional AMSC conducted a RAD/NUC Detection Seminar. The scenario focused on a RAD/NUC incident occurring during a large marine event on the Ohio River in the Port of Louisville. The exercise evaluated components of the Ohio Valley Maritime RAD/NUC Detection Concept of Operations Plan (CONOPS), and educated AMSC members on a RAD/NUC response in the regional area. Due to COVID-19, in-person participation was limited to no more than 30 participants. The Homeland Security Information Network (HSIN) Connect virtual meeting room was employed to maximize attendance.

Maritime Domain Awareness: Sector New York is working with Sector Long Island Sound on an offshore windfarm project that will span across both COTP zones. The FMSCs are establishing the necessary relationships with port partners to obtain a full scope of the project, including landside support facilities, as well as the waterside installations and locations as they relate to the safety and security of both AOR's Maritime Domain.

Arctic Regional Security Workshop: Western Alaska AMSC participated in the two-day Advancing Collaboration in Canada-U.S. Arctic Regional Security Workshop, which explored the current reality and future of Arctic security and defense from a North American perspective. Bringing together a diverse array of experienced and knowledgeable practitioners and academics, the workshop considered Arctic issues holistically, drawing out and highlighting the interconnected web of challenges and opportunities that underpin and frame actions in a Northern context.

Port Protector AMSTEP Workshop: The Central California AMSC conducted its annual “Port Protector” AMSTEP exercise in December 2020. The exercise was originally scheduled as a Tabletop Exercise (TTX) to discuss a scenario on a contagion aboard an inbound cruise ship. However, they changed the scope to a “Pandemic Lessons Learned Workshop” and focused on five separate components of the maritime industry. Subject matter experts from across the country contributed the lessons learned from their respective organization and their industry.

AMSC Partners Support of Real World Events (RWEs): Maryland-NCR AMSC port partners assisted in a number of security RWEs in 2020. The AMSCs Maritime Tactical Operators Group (MTOG) and Intel subcommittees assisted with the Ocean City Air Show. During the 4th of July weekend, several members of the MTOG subcommittee assisted with providing safety and security to the waterside events planned. Additionally, several AMSC MTOG subcommittee members assisted with the 4th of July events near the nation’s capital. Each RWE bolstered interagency communication and coordination.

Training Partnerships: Delaware Bay AMSC Executive Secretary developed partnerships with training officers from the three states within their COTP Zone (DE, NJ, and PA) The New Jersey Office of Homeland Security and Preparedness (NJOHSP) and Delaware Bay AMSC co-sponsored two sessions of FEMA’s “AWR 144: Port and Vessel Security for Public Safety and Maritime Personnel” training. With the assistance of Pennsylvania’s Training Officer, Delaware Bay hosted the DHS/FEMA MGT-385 Community Cybersecurity Exercise Planning course. All three states spanning Sector Delaware Bay’s area of responsibility collaborated to share additional virtual training opportunities with the AMSC membership. Although some training was not specifically exclusive to the maritime domain (e.g., Active Shooter), 22 security related sessions were offered to port members at no cost.

AS/AT Exercises and Drills: Southeastern New England AMSC facilitated an AT Response Virtual Workshop in 2020. The focus was plans and procedures to respond to an AS incident to a passenger ferry operating in Vineyard Sound. Procedures were also discussed on a newly designed boarding ladder that expedites the embarkation of the responding agency personnel.

Ohio Valley AMSC's Cincinnati Regional AMSC Subcommittee conducted an AS TTX using a combination of in-person and virtual through the HSIN Connect online platform.

Puget Sound AMSC Public Safety and Law Enforcement AMSC Subcommittee executed three Alert Warning System drills to test the preparedness and response of partners in the event of an AT onboard the Washington State Ferry or other High Capacity Passenger Vessel.

Western Alaska AMSC partnered with a representative from DHS CISA to facilitate an AS training workshop for AMSC members.

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 2020.

Cybersecurity. The majority of the AMSCs have established cyber subcommittees to address cybersecurity risks. Many of these subcommittees reported increased participation from port partners in 2020. The Port of New York and New Jersey AMSC along with sector personnel attended a meeting with the USCG Cyber Protection Team[2] (CPT). Port partners introduced to the CPT have started to use their services of assess, hunt, clear, and harden. Northern New England's AMSC is working with the University of Maine to develop IT cybersecurity training for port partners. The Houston-Galveston AMSC cybersecurity subcommittee partnered with the FBI's InfraGard[3] division to share best practices, lessons learned and timely information with their maritime stakeholders. Elements within each of the Sector's AMSCs are exploring opportunities and developing regional strategies to enhance cybersecurity across information sharing platforms within their local and state networks, and developing cyber-related exercises within their port-wide areas.

COVID-19. AMSCs used alternative means to communicate information to their port partners during the COVID-19 pandemic. Sector New York conducted bi-weekly conference calls to share information on how the pandemic was impacting the maritime community, the MTS, and the economy. Maryland-NCR AMSC members received a monthly newsletter keeping them updated

[2] https://www.dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/

[3] https://www.infragard.org/

on subcommittee activities, Intel and cyber updates, public and private maritime business impacts, and dates of upcoming virtual training and meetings. Despite the constraints COVID-19 placed on Charleston AMSC members, the Sea Hawk Interagency Operating subcommittee continued to conduct multiagency operations. Sault Region AMSC maintained relationships with the local emergency managers to maintain situational awareness of local concerns.

Multi-Agency Strike Force Operations (MSFOs). The Central California AMSC members joined federal, state, and other local port partners in conducting MSFOs. These efforts have increased the scope of container inspections from hazardous materials regulatory compliance to include emphasis on chemical, biological, radiological, nuclear, explosive, and weapons smuggling. Additionally, the team looks for Global Positioning System jamming and spoofing equipment in truck cabs, which may inadvertently block signals used by ship navigational systems.

Virtual Platforms. Maryland-National Capital Region (NCR) AMSC Executive Secretary relayed that the COVID-19 restrictions hampered in-person meetings. They used a variety of virtual platforms to conduct meetings (Microsoft Teams, WebEx, etc.), which allowed AMSC members to still attend. The Port of New York and New Jersey AMSC and the Northeast and Eastern Central Florida AMSC both used the DHS HSIN Adobe Connect virtual platform in 2020 to conduct their PSGP field reviews. Puerto Rico and the Virgin Island AMSC preferred to use Microsoft Teams as it assisted in maintaining partnership and cohesion throughout the pandemic. Many AMSCs stated AMSC member participation increased using virtual meeting platforms, but most reported their members prefer in-person meetings.

AT Planning and Exercises. The Boston AMSC tested their AT CONOPS during a functional exercise. Valuable updates and edits to the plan included changing the tactical frequencies used by all responders, updating the 911 dispatch notification lists/protocols, and introducing a wider range of text alerts. Southeastern New England AMSC hosted a number of AT Response Plan workshops, focusing on post-event action considered essential to mission success. Delaware Bay's AMSC Maritime Tactical Operations Working Group assisted in the development of a new AT Response Plan which will be tested during a scheduled exercise in 2021. Ohio Valley AMSCs conducted an AS TTX in preparation for an operations based exercise scheduled in 2021.

AMSC Briefings. The South Louisiana AMSC Executive Secretaries facilitated bi-weekly Virtual Interagency Operations Center briefings between MSU Houma, MSU Morgan City, Customs and Border Protection (CBP) and CBP-Office of Air and Marine. These briefings enhanced Maritime Domain Awareness and acted as force multipliers by increasing joint boarding operations and associated arrests/detentions throughout the COTP Houma zone. The briefings included topics on vessel arrivals/departures, crew makeup, cargo, patrol and inspection schedules, and suspicious activity aboard vessels.

Port Assessment Team Survey. In order to improve efficiency and manage expectations of post-incidents (e.g., from a Transportation Security Incident), Sector Hawaii staff standardized the team composition, process and deliverable system of the post-incident surveys. This now allows for improved decision-making by the Incident Command Post and sharing of the information to other Emergency Operations Centers. The skills required for the team were developed by a multi-agency group and tested as part of an operation exercise. The final procedure was incorporated into a pre-incident ICS 204 form.

6.0 Headquarters Input

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

Cyber. Coast Guard Headquarters continues to develop guidance and other resources to address cyber safety, security, and cyber risk management within the MTS. CG-FAC oversaw the 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. 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, as well as engage with their local Coast Guard office. In addition to the NVIC, CG-FAC maintains a publically-available frequently asked questions document and also released a Facility Inspector Cyber job aid to provide marine safety personnel with additional support tools as they address facilities' documented cyber vulnerabilities.

The Coast Guard also continued efforts to increase cybersecurity/cyber risk management proficiency in the MTS through training. Program offices at headquarters are working together to develop cyber training for the field, including a Learning Management System-based module, a Stevens Institute course, and combined CG-FAC/CGCYBER/CG-791 virtual and roadshow workshops.

In response to Congressional direction in the FAA Authorization Act of 2018, CG-FAC led efforts in the development of a Maritime Cyber Risk Assessment Model (MCRAM) through engagement within the Coast Guard, partner agencies, and maritime stakeholders. The MCRAM leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework and will be a tool for individual facilities, companies, or ports/harbors to conduct basic cyber risk self-assessments on where they stand in regards to mitigating cyber risks. It allows the user to prioritize based on their own determination of specific business needs, priorities, and resources. This model is intended for use by MTS stakeholders ranging from port authorities to AMSCs (and Cybersecurity subcommittees), to individual facility owners/operators/security officers.

UAS. Coast Guard Headquarter Program Offices continue to participate in DHS UAS working groups. For example, there is a legal working group currently focused on the reauthorization of C-UAS authority under 6 U.S.C. § 124n, which sunsets in October 2022. Additionally:

> Section 2209 of FAA Extension, Safety, and Security Act of 2016 requires the Secretary of Transportation to establish a process to allow certain fixed-site facility owners or operators to petition the FAA to prohibit or restrict the operation of unmanned aircraft in close proximity to certain facilities, such as national security sites, critical infrastructure, amusement parks and other locations, that warrant such a restriction.[4]

This process is currently under development. CG-MSR prerecorded a UAS video presentation, followed by participation in a UAS panel discussion at the recent PSS Virtual Workshop. The following are some of the updates the participants were briefed on:

- USCG does have deployable capability with limited capacity per the Preventing Emerging Threats Act (PETA) of 2018.
- CG C-UAS is currently a pilot project and in process of becoming a program.
- The 2020 National Port Readiness Network has an action item addressing UAS threat to Military Outload (MOL) Operations.

The USCG UAS Community CG-Portal page (internal) continues to provide resources and latest developments. FAA Law Enforcement Assistance Program office has a public safety and law enforcement toolkit[5] available to assist in operating and handling situations involving UASs.

Virtual Environment. In 2020, the AMSCs had to quickly adapt to facilitating virtual meetings in lieu of in-person meetings due to the COVID-19 pandemic. The AMSC Executive Secretaries noted that their port stakeholders were successfully using virtual platforms, but most of these platforms were not authorized on their government workstations. A new list of recommended

[4] https://www.federalregister.gov/d/2019-00758/p-39

[5] https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit/

Coast Guard virtual platforms was published in April. A link was also provided to a DOD repository of other acceptable virtual platforms. Program offices will continue to monitor connectivity issues and provide updated resources for successful outreach and collaboration efforts with our port partners.

AS/AT. CG-MSR established a "C" school to train personnel in Active Shooter response tactics by teaming up with Texas State University's Advanced Law Enforcement Rapid Response Tactics (ALERRT) program to assist the Coast Guard in creating a similar program that would met the CG needs while making CG responders interoperable with OGA partners. The Boarding Officer Offshore Course is slated to become available online. An electronic version of Tactical Procedures and AS/AT Response CG Tactics, Techniques, and Procedures is under development and will further assist with training CG resources. AMSCs continue to work with port stakeholders and LE subcommittees to plan for multi-agency responses to potential AS/AT maritime incidents.

MTS Resilience/Recovery. The 2020 hurricane season was the most active and fifth costliest hurricane season on record. In total, there were thirty named storms, with thirteen that developed into hurricanes. Twelve storms made landfall in the contiguous U.S. breaking the previous record of nine set in 1916. September was the most active month on record with ten named storms. These storms resulted in over $60 billion[6] in damages. The impact of Category 4 hurricanes Laura and Delta, as well as Tropical Storm Beta, in quick succession inflicted unrelenting damage on the Texas/Louisiana border, creating facility closures and delays in many deep water ports that facilitate billions of dollars of economic activity. Hurricane Eta, a Category 4 hurricane, caused widespread power outages in Florida and over 10 inches of rainfall in certain areas of North and South Carolina.

Emergency Support Function-1 watch standers worked quickly to consolidate information and communicating to senior leadership, enabling them to take necessary action to mitigate impacts to the Maritime Transportation System. The COVID-19 pandemic provided additional complexities to already dynamic response efforts. Overcoming these challenges were the result of outstanding work by local Marine Transportation System Recovery Units (MTSRUs) and communication between all levels of command. Senior leaders in FEMA, the Department of Transportation (DOT), DHS, and CG were well informed of the status of vital ports and directly attributed to the development of viable alternatives to enable the flow of relief efforts. The CG recognizes the value of collaboration and continues to encourage cooperation with federal,

[6] https://www.accuweather.com/en/hurricane/record-breaking-2020-hurricane-season-caused-60-billion-to-65-billion-in-economic-damage/858788

state, local, tribal, and territorial officials, and our industry port partners to support MTS safety, security, and resilience.

Soon after COVID-19 became a public health crisis within the United States, the CDC issued the initial 30-day No-Sail Order for cruise ships on March 14th, 2020. The Coast Guard activated its MTSRU Support Cell (MTSRU-SC) in order to measure the impact of COVID-19 and policy measures on the maritime industry. The general focus was on cruise ships and the impact of the No-Sail Order. In March of 2020, there were over 250,000 passengers and 60,000 crewmembers aboard cruise ships. Coast Guard and industry worked together to disembark passengers and nonessential crewmembers in the weeks following the No-Sail Order. When the CDC issued a Framework for Conditional Sailing Order and subsequent updates, the MTSR-SC tracked various metrics, such as the locations of cruise ships, their anticipated restart date for sailing with passengers, their crew numbers, and their arrival into U.S. Ports. Their products were used to inform Coast Guard leadership and multiple stakeholder groups including the CDC, National Oceanic and Atmospheric Administration, the Committee on the MTS COVID-19 Working Group, DOT, and other government agencies.

7.0 Conclusion

AMSCs are absolutely vital to securing the MTS. Through collaboration, innovation, information sharing, and regular engagement, AMSCs serve as the focal point for government and industry security coordination at the local level. They play a critical role in maintaining a strong security posture while also spotlighting new risks and emerging threats that could have cascading effects in the MTS. AMSCs directly impact the Nation’s economic and national security.