Area Maritime Security Committee

Challenges, Suggestions, Accomplishments, and Best Practices

2023 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

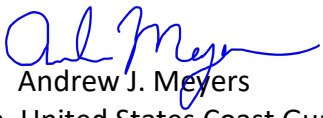
Office of Port and Facility Compliance (CG-FAC)

Office Chief's Perspective

The Marine Transportation System (MTS) supports $5.4 trillion of economic activity each year and supports the employment of more than 30 million Americans. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. 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.

Area Maritime Security Committees (AMSCs) serve an incredibly valuable role as focal points for local and 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 MTS. They are a key component of the layered security that is necessary to protect our MTS from the diverse threats it faces.

The AMSC annual report is a valuable resource for sharing 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, and AMSC relationships and actions are critical to addressing the emerging threats and complex challenges facing the maritime domain.



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

1.0 Background

The AMSCs are 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 within federal, state, local, tribal, and territorial government, and private sector stakeholders to address security issues impacting the maritime domain. The Captain of the Port (COTP) establishes and directs the AMSCs through their designation as the Federal Maritime Security Coordinators (FMSCs). Each year, the AMSCs report their challenges, accomplishments, best practices, and recommendations to ensure the Coast Guard and maritime communities remain aligned with national preparedness goals and to improve AMSC effectiveness nationwide.

2.0 Challenges

Enclosure (1) identifies all challenges reported from each AMSC in 2023. The following highlight common themes:

AMSC Participation.

- Federal government funding uncertainties greatly affected the ability to proactively plan and schedule AMSC meetings, exercises, and training.
- AMSC members familiarity with some segments of the AMSP during real world events and exercises was lacking even though they had access to the plan.
- Geographical challenges existed for some AMSCs where COTP zones encompass large Areas of Responsibility (AOR). Outreach to some AORs were impeded by staffing shortages.

Cybersecurity and the MTS.

- More guidance and examples needed on what constitutes a Cyber Transportation Security Incident.
- Not all Sectors have been able to fill the Marine Transportation System Specialists-Cyber (MTSS-C) positions as demand for cybersecurity specialists was greater than the current pool of available applicants.
- AMSC members representing MTSA regulated waterfront facilities face challenges of implementing effective cybersecurity measures due to a lack of resources, expertise, visibility, and understanding of the complex issues involved.

Unmanned Aircraft Systems (UAS) access to the MTS.

- Managing UASs security issues were challenging when they flew over port facilities at low altitude, as neither facility management nor the Coast Guard had jurisdiction over UASs while they were airborne.
- Worldwide media has highlighted the effectiveness of drones used as weapons. There does not appear to be any guidance on how our port partners can prevent, intercept, or mitigate this type of threat to maritime targets.

Homeport 2.0. Homeport is a critical tool for AMSCs to effectively share Sensitive Security Information (SSI) with AMSC members.

- Homeport 2.0 was underutilized by AMSC membership, though adequate use for facility and waterway issues. AMSC members perceive Homeport as outdated and not user-friendly.
- Homeport was not an effective tool for organizing port security information, which further deterred AMSC members from seeking information on this platform.

Port Security Grant Program (PSGP). The grant program allocates funds based on risk to implement the AMSPs among port authorities, facility operators, and state and local government agencies required to provide port security services and to train public safety personnel.

- Each year, the Federal Emergency Management Agency's (FEMA) port security grants seemed to be increasingly dominated by state and local partners who have a 25% match, while grants from industry partners, have a 50% match requirement resulting in fewer investment justifications submitted. Within the AMSC, this "unequal" cost share appeared to be a disincentive for MTSA partners to apply.
- There was a concern that further reduction or possible elimination of PSGP funding could leave some marine response agencies utilizing response boats well outside their operational life cycle.

Active Shooter/Active Threat (AS/AT). The growing number of AS/AT occurrences compels committees to be prepared for an incident in the maritime domain.

- Addressing and responding to an AS/AT scenario aboard a High-Capacity Passenger Vessel, especially ferries, remained an ongoing and formidable challenge to AMSCs.

3.0 Suggestions

The AMSC reports identified many helpful and practical suggestions highlighted below. Enclosure (2) identifies suggestions reported from each AMSC in 2023:

Cybersecurity/Cyber Risk Management.

- Some port partners who represent national or regional companies often manage cybersecurity outside the COTP zone, which in these instances made it difficult to bridge collaboration between the physical security personnel and the cybersecurity personnel.
- Training provided on artificial intelligence theory, application, and limitations on what it can and cannot do regarding the MTS would be beneficial.
- Develop a Cybersecurity Training, Tactics, and Procedures guide that provides standard procedures for response and information sharing to port partners in the event of a cyber incident.

Homeport 2.0.

- Many suggested the issues with Homeport need to be addressed and if they could not, then another more efficient platform to use should be provided.
- A reoccurring suggestion was to allow port stakeholder accounts to be reset at the Sector level. Users need quick access to Homeport during an incident without having to contact the help desk.

UAS.

- AMSCs suggested pursuit of new technology and training is needed to address not only UAS threats but also emerging threats from Unmanned Underwater Vehicles (UUV).
- The use of UUVs is expanding in the maritime domain. The USCG should address the regulatory, operational, and security challenges associated with these systems and develop protocols to ensure compliance with existing regulations.
- Consider leveraging local Counter Unmanned Aerial Systems (C-UAS) to use for special events and to pre-establish C-UAS Memorandums of Understanding (MOU) with local and state authorities.
- Suggest that the Coast Guard continue to work with the Federal Aviation Administration (FAA) to update the FAA Extension Safety and Security Act of 2016 for C-UAS policy and guidance.

AS/AT Incidents.

- Develop policies that address AS/AT in a maritime environment as it is a major concern for ferry systems.
- Active shooter (AS) incident on a High-Capacity Passenger Vessel underway guidance is needed and a list of available resources to utilize and prepare for this type of event.

PSGP.

- Continue to support stakeholders on the process for FEMA Grant applications due to personnel turnover and updates in the notices each year.
- Transparency in the Port Security Grant request reviews.
- AMSCs suggest the need for mandated life-cycle support of equipment and infrastructure procured with PSGP funds.

4.0 Accomplishments

In 2023, AMSCs and their respective subcommittees facilitated 1,772 events. This total included 1,018 administrative AMSC meetings (e.g., Executive Steering Committees and General AMSC meetings) and 754 training events (includes 103 joint agency training meetings, 465 maritime security training operations, 107 training exercises, 46 Incident Command System [ICS] training sessions, and 33 MTS Recovery Unit [MTSRU] training sessions). These coordinated opportunities resulted in effective, real world security prevention, response, and recovery efforts. Enclosure (3) identifies accomplishments reported from each AMSC.

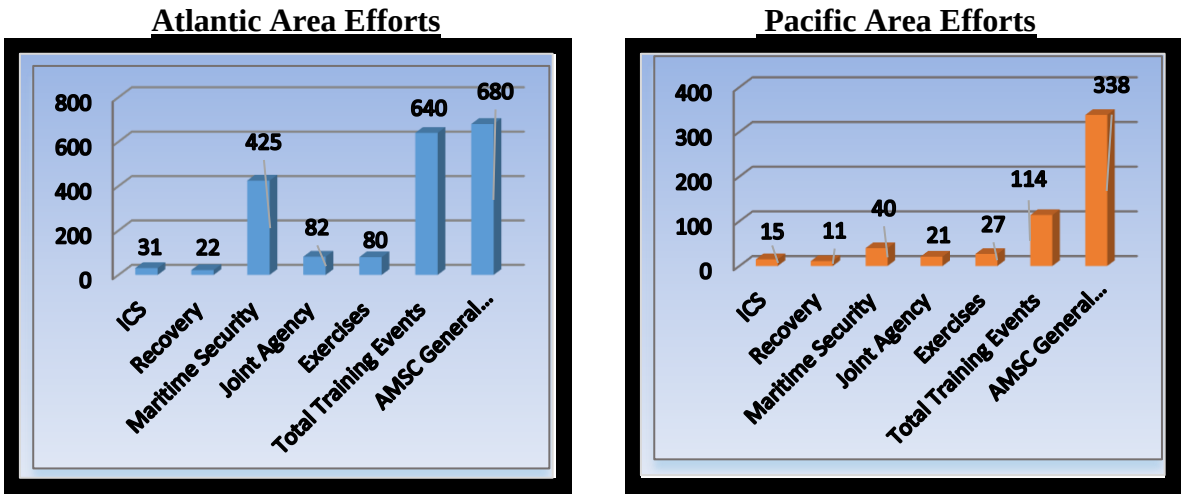


Figure 1 – AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners and stakeholders that do not fall into the ICS, Recovery, Maritime Security, Exercises or Meetings categories; Exercises include all Tabletop Exercises (TTX), Functional Exercises (FE), Full Scale Exercises (FSE) and drills; Meetings are tallied from each AMSC. (Atlantic Area covers 32 AMSCs and Pacific Area covers 11 AMSCs.)

Cyber. The importance of cybersecurity continues to highlight global and national cyber events. Port stakeholders are more engaged and request relevant maritime cybersecurity information to be passed through appropriate channels to them. Noteworthy AMSCs cybersecurity accomplishments include:

- Charleston AMSC co-sponsored an Area Maritime Security and Training Program (AMSTEP) Cybersecurity TTX with the Transportation Security Administration (TSA)

Intermodal Security Training and Exercise Program (I-STEP) exercise team on August 9, 2023. This exercise proved critical in improving coordination between federal, state, and maritime industry partners in preparation for a cyber-attack incident response. Lessons learned from this exercise greatly enhanced the new AMSP Cybersecurity Annex.

- Within the Cybersecurity mission area, the Virginia AMSC Cybersecurity Subcommittee benefitted from the new civilian assigned as Sector Virginia's MTSS-C. Under his guidance, the AMSC Cyber Subcommittee is completing the five-year update of their Cyber Incident Response Plan (CIRP), as well as topics and content necessary to keep their AMSC members current on the latest cybersecurity measures and procedures. The Cyber Subcommittee continued work on refining their charter as well and aided the D-5 MTSS-C in planning a future "Cyber Cascade" TTX and a FSE "CYBER FORTRESS" with the Virginia National Guard. Both exercises will provide a solid test of their overall cyber readiness and a new Command Center Cyber Quick Response Card (QRC).
- Six successful USCG Cyber Protection Team (CPT) Assessment and Hunt Missions were conducted at port facilities across the Puget Sound Region, with a specific focus on three designated military strategic ports. These efforts significantly enhanced the resilience of shore-side security for the MTS. As a result of these assessments, facilities submitted requests for FEMA Port Security Grant funds, directly addressing vulnerabilities uncovered during the CPT assessments. The cyber posture of MTSA-regulated facilities in the region has steadily improved through active participation in AMSC Cybersecurity Subcommittee meetings and related activities, including targeted public education efforts by the Sector's MTSS-C aimed at the MTS community.
- The Maritime Cybersecurity Outreach Tool (COT) is a 101-crash course for the New York and New Jersey AMSC's port partners to learn the broad aspects of cybersecurity, the associated threats, methods to ensure each organization's effectiveness in combatting these threats, and tools to ensure recovery from varying cyber-attacks. The COT provided port partners with current data regarding past threats which were successful as well as those blocked or mitigated by the USCG CPT. Hyperlinks contained within the COT provided port partners valuable self-assessment tools to determine vulnerabilities. These tools provide the port partners extraordinarily value in safely challenging their digital landscape and to successfully fortify weak points in cybersecurity. The COT provided direct contact information for the CPT, which stands ready to assist any of our port partners and to conduct assessments free of charge.

Panama Reciprocal Engagement. In January 2023, Sector New Orleans hosted the Panama Reciprocal Engagement. This initiative was driven by the similarities between New Orleans Port Area and the Panama Canal Zone. The Panamanian Delegation consisted of members of the Panama Ministry of Public Security, National Aeronaval Service, Canal Authority, Maritime Authority, Phoenix Marine, as well as members from the U.S. Embassy.

The Executive Secretary of the AMSC, in collaboration with representatives from the U.S. Coast Guard's International Port Security Program and the U.S. Embassy, designed a two-day itinerary that addressed the delegation's primary objective by providing a firsthand look at how the AMSC effectively integrates government entities (federal, state, and local) and industry together under a common structure and purpose. The delegation participated in key AMSC meetings, visited similar industries and facilities, and engaged in discussions with stakeholders to witness the effective coordination of authorities, responsibilities, and capabilities to advance port and maritime security goals. Additionally, the delegation attended the AMSTEP and the Louisiana Maritime Security Community (LOMSEC) Subcommittee Communication and Response Exercise, further solidifying their admiration for the synergy among government agencies, port partners, and stakeholders in the area. Inspired by this event, the delegation is now pursuing the development of their own scenario-based exercise, with the support of the U.S. Embassy and the Panama Ministry of Public Security personnel working alongside the Center for Naval Analyses (CNA). This exercise, scheduled for October 2024, will be focused on Canal security.

UAS.

- Central CA AMSC had assistance from the Maritime Security Response Team East (MSRT-E), who provided C-UAS support to the nation's most attended airshow at Huntington Beach (750,000 spectators). Their team successfully detected 15 drones violating the Temporary Flight Restriction (TFR); electronically mitigated six UAS assessed as a threat; and interdicted seven UAS operators with the assistance of the Huntington Beach Police Department (HBPD) and FAA Law Enforcement Assistance Program (LEAP) officer. Notably, this was the first integration of FAA LEAP officer during a MSRT-E C-UAS Ops evolution and the coordination worked well.
- The North Carolina AMSC achieved a significant milestone by establishing an UAS Subcommittee. This forward-thinking initiative represents a major advancement in maritime security and emergency response capabilities for coastal North Carolina. The UAS Subcommittee was tasked with integrating drone technology into maritime security operations, providing an innovative and efficient approach to surveillance, inspection, and emergency situations. This development not only enhanced the operational effectiveness of the CG Sector North Carolina but also positioned it at the forefront of adopting innovative technologies in maritime security. This subcommittee already had a positive effect on CG operations. For example, during a recent Nor'easter which caused multiple vessels to break free from moorings and ground/sink in the Atlantic Intercoastal Waterway the subcommittee was able to supply real time observations to help operational commanders make rapid and informed decisions to limit environmental damage and MTS disruptions.
- Long Island Sound (LIS) port stakeholders assisted with a coordinated investigation to identify a UAS operator who was responsible for nine unauthorized operations in the

vicinity of MTSA-regulated vessels with the Cross Sound Ferry System. The operator was identified and cited for negligent operations. Six public agencies were involved with the investigation, to include TSA, FAA, Connecticut State Police, Naval Criminal Investigative Service (NCIS), Coast Guard Investigative Service (CGIS), and Sector LIS.

Unmanned Surface Vessel (USV) FSE. The San Diego AMSC hosted its 2023 Unmanned Surface Vessel (USV) FSE on September 26th, 2023. More than 65 participants from 14 local, state, and federal agencies, along with two prestigious universities came together to plan, participate, and provide analysis on testing port partners' ability to detect and respond to an USV threat as a Waterborne Improvised Explosive Device within the Port of San Diego. This exercise laid the foundation for a heightened threat level and ensured additional detection capability equipment was implemented in the exercise, provided a platform to simulate a "real-world" threat with actual USVs operating on the water. This exercise was guided by objectives to test sensor capabilities to detect an USV threat at the entrance to San Diego Bay, evaluated on-water and land response actions by law enforcement and government agencies, and evaluated the utility and accuracy of laydown locations to render safe Waterborne Improvised Explosive Devices. The AMSC will be able to implement measures to improve communications, update the AMSP, and enhance collaborative agency response procedures to effectively neutralize this type of threat in the future. The exercise was highlighted in a publicized article within Sea Power and Ocean Robotics Planet magazines and websites. The After-Action Report (AAR) has been requested by multiple DoD/DHS agencies. Also, USCG HQ Program Office requested the AAR as a foundation for the National Security Council Counter-Unmanned and Autonomous Maritime System National Action Plan.

Shipboard Firefighting. Sector Lake Michigan had used recent case information and lessons learned from a major shipboard fire in a local shipyard and winter lay-up location to further discussions about commercial firefighting. The Sector used the local AMSC as a springboard to inform all the AMSCs members on firefighting capability gaps which eventually became a Great Lakes Initiative with the assistance of USCG District Nine.

Hawaii and American Samoa AMSC Tsunami Workgroup. In coordination with the National Tsunami Hazard Mitigation Program (NTHMP), the workgroup continued maritime hazard modeling/mapping of Hawaii, Maui, and Kauai Island harbors for long-term infrastructure planning in support of Hawaii DOT-Harbor's Master Plan 2050.

Two Active Threat (AT) FE. The Boston AMSC AT Subcommittee, in coordination with personnel from Sector Boston, conducted two simultaneous FEs on October 25, 2023, aboard two underway ferries. One ferry conducted a 15-vessel boarding exercise, while the second ferry conducted an Unmanned Aerial Vehicle (UAV) launch/retrieval to video the ongoing threats for situational awareness. Crews were tested on their ability to communicate/coordinate, demonstrated

alongside approach, then board/cleared an underway passenger ferry with ATs onboard. Additionally, a robotic dog was onboard to identify potential threats while an autonomous 24-foot safe boat was underway to identify and retrieve persons in the water. This exercise received media attention via industry publication in the Foghorn Magazine. Port Partners served as observers and evaluators for this exercise.

AMSC Members Support Role. The South Texas AMSC committee members continued to serve a pivotal role in supporting the South Texas Project Nuclear Operating Company on the Colorado River. Committee members served on the Incident Management Team for the Plume Exposure Pathway FE in Bay City, TX in August 2023.

Port Risk Analysis Model (PORT-RAM). The Western Florida AMSC in conjunction with the AMSC Executive Secretary worked with FEMA and the Tampa Port Authority using Port Tampa as a beta-test subject for PORT-RAM. Tampa is one of four ports nationally (Port of Los Angeles, Port of Long Beach, Port of Hampton Roads, and Port Tampa) to volunteer for PORT-RAM as a test subject which contributed to its accreditation and to justify Port Security Grant Investment Justifications. As Congress closely scrutinizes the PSG Program, FEMA needs to provide metrics to reflect measurable prevention and return on grant investment. The port leveraged the Port Security Specialist's knowledge and experience and the Maritime Security Risk Analysis Model (MSRAM) to accomplish this three-day data collection/risk picture assessment.

AS/AT Exercises and Drills.

- Bay Ferry VI was a regional FSE sponsored by the Golden Gate Transportation District (Golden Gate Ferry) using PSGP funding obtained with the assistance of the Northern California AMSC. The four-day exercise concentrated on four key maritime vulnerabilities; 1) a threatened radiological release in the San Francisco Bay port region, 2) an AS aboard a docked ferryboat, 3) an AS aboard an underway ferryboat, and 4) the rescue and management of survivors following an AS and bombing aboard a ferryboat. The overall exercise consisted of numerous planning meetings, a TTX in August 2023, the four-day FSE in September 2023 and the development of an AS/AT "template-plan" for use by the region's ferryboat companies as a supplement to their MTSA security plans.
- To buy down risk associated with a maritime AS/AT scenario in the Straits of Mackinac, Sector Northern Great Lakes and the Mackinac County Sheriff's Office have entered an MOU to enhance ferry security operations. This was a significant milestone in the AMSCs efforts to reduce various security vulnerabilities in the region's busy passenger ferry industry. The purpose of this MOU is to set forth policies, procedures, and responsibilities regarding USCG Law Enforcement and security operations conducted in conjunction with the Mackinac County Sheriff's Office at Mackinac Island ferry terminals or onboard underway Mackinac Island ferries.

- Western Florida AMSC partnered with Cybersecurity and Infrastructure Security Agency's (CISA) Exercise Support Team to create and facilitate the 2023 AS/AT AMSTEP. This effort strengthened the USCG/CISA partnership and resulted in three exercise planning meetings, a detailed exercise situation manual, and exercise facilitation by CISA Exercise Support, Regional DHS Protective Security Advisor (PSA) and the AMSC Executive Secretary. This imparted positive partnership optics on exercise participants and served as an excellent opportunity to exploit training/exercise resources/capabilities.

5.0 Best Practices

Enclosure (4) identifies best practices reported from each AMSC in 2023. Below were highlights of specific programs, concepts, and initiatives.

Cybersecurity. Cybersecurity risks are addressed through AMSC Cybersecurity Subcommittees.

- Ahead of the 2024 validation cycle for the Area Maritime Security Assessment (AMSA) and the AMSP the Western Florida's AMSC Executive Secretary collaborated with the MTSS-C and the Facilities Compliance Branch to evaluate the AMSC related port operations.
- The New Orleans and Baton Rouge AMSCs quickly learned after an AMSC Cybersecurity Subcommittee was established, that having this subcommittee with diverse representatives from across federal, state, industry, and academia was extremely helpful in providing up-to-date information on cyber threats across the region and nationally. An AMSC Cybersecurity Subcommittee with similar diverse representation should be a best practice across all AMSCs.
- During the Saint Louis AMSC planning process for the 2023 cybersecurity exercise, it became clear there is often an awareness gap between Information Technology (IT) staff and traditional emergency planners and security personnel. As planning staff posed questions about various security scenarios coupled with potential cyber-attack vectors, the planning team identified several potential vulnerabilities the IT staff were able to address within their operations before the day of the exercise. Emergency planners/responders and IT professionals must develop closer relationships within their organizations to foster a holistic approach to risk management from both physical and cybersecurity perspectives.
- Members of the San Diego AMSC Cybersecurity Subcommittee proposed to the Executive Steering Committee (ESC) a semi-annual scenario discussion with senior leadership on a cyber-attack to the Port of San Diego region. This was discussed and accepted. The scenario and discussion questions were sent to senior leaders of agencies/organizations that attend the AMSC prior to the meeting convening. The scenario discussion was facilitated by members of the Cybersecurity Subcommittee. The purpose, objectives, discussion rules, and module layout were explained to attendees. As the scenario

unfolded, each module concluded with a set of questions to get senior leadership thinking of what actions they would take, what information they expect to share with port partners, and what their priorities would be. The discussion concluded with a hot wash on what is each organization's top priority in responding to this incident and what cybersecurity training would the AMSC like the Cybersecurity Subcommittee to focus on in the future. This also will be one of the mechanisms to assist the AMSC in determining the strategic economic impact and national security posture if a cybersecurity incident or any other event impacting the MTS, prohibiting vessel traffic from entering or exiting the Tier 1 strategic military Port of San Diego for hours or days.

- The Western Alaska AMSC cyber team has expanded their outreach efforts to include a focus on executive level audiences expounding on the holistic role of cybersecurity as part of improved resiliency for a business model. Recent success includes a presentation to the Lieutenant Governor of Alaska.

UAS Subcommittee. The Houston/Galveston AMSC UAS Subcommittee has over 30 members. The subcommittee has continued to mature and boaster the security of their AOR as the number of suspicious drone sightings over MTSA facilities and critical infrastructure has continued to grow.

Marine Fire Fighting.

- The New York and New Jersey AMSC worked with port partners and with the New York Fire Department to train with their Marine Shipboard Firefighting Simulator (awarded through the PSGP process). The simulator is available to local, state, and federal emergency responders, to include U.S. Coast Guard personnel.
- The Charleston AMSC noted having the Salvage and Marine Fire Fighting Subcommittee as a joint subcommittee consisting of both AMSC and Area Committee members ensures all equities are considered and proper coordination when planning is conducted.
- In August 2023 the Ohio Valley AMSC conducted marine firefighting training. The training focused on response to a commercial vessel or facility fire and was provided at no cost to over 60 regional fire agencies and maritime industry fire department personnel.
- Inclusion of a Marine Firefighting Task Force was introduced to members during recent Southeast Michigan AMSC subcommittee meetings. Members were provided with briefings from District 9, District Response Advisory Team, which provided an update to marine firefighting with emphasis on coastal or pier-side motor vessels suffering a large fire casualty. A large percentage of committee members who are first responders expressed interest in joining the task force to train and respond appropriately. An exercise is planned for 2024 which will further enhance training and potential multiagency response needed for catastrophic vessel fires along heavily populated communities within all Sector Detroit port areas.

AS/AT.

- The Northern New England AMSC was able to conduct several Active Shooter exercises across several venues. Through collaboration with local and state agencies, a series of FSEs and TTXs were successfully executed at both Sector facilities and Rockland Ferries. These engagements bolstered relationships with law enforcement partners and first responders.
- During the Central California AMSCs Port Protector 2023 AMSTEP, participants discovered that the advantage posed by an airborne (i.e., helicopter) designated marksman, would dramatically assist the ability of USCG/LE forces to gain access to an AS/AT vessel.

Best Practices Highlights.

- Over half of D-8 AMSCs reported the use of a managing or steering body, which included key stakeholder representatives that met annually to provide direction for future year AMSC activities. Meetings of these bodies increased stakeholder buy-in and provided opportunities for the body to consider topics including threat and capability assessments, Coast Guard strategic direction, and stakeholder needs and priorities. Leveraging partnerships between the Coast Guard, the AMSC, and other agencies, professional associations, and committees to further maritime security goals continued as a key driver of success in CY23.
- During Admiral Fagan's visit to Panama in August 2023, Panamanian officials praised the New Orleans AMSC as a prime example of best practices for enhancing security in the maritime environment. Recognizing the effectiveness and collaborative nature of the New Orleans AMSC, the Panamanian Delegation engaged in strategic meetings with key stakeholders, including the U.S. Ambassador and the Panamanian Minister of Public Security. Their objective was to establish a coalition for the creation of their own AMSC-like coordinating body to create collaborative approach to securing the Canal Zone. Sector New Orleans willingly provided the U.S. Embassy with a redacted AMSC charter to assist the Panamanians in identifying the committee's purpose, responsibility, objectives, order of business, records, and rules of membership. This was a perfect example that by its continued dedication, strategic approach, and proven success, the New Orleans AMSC remains a steadfast leader in the field, setting the standards for maritime security excellence.
- The South Texas AMSC members continued its strong historical engagement with several local and regional coordination groups, including ASIS International, Coastal Bend Regional Advisory Council, Coastal Bend Emergency Management Association, Port Industries of Corpus Christi, Coastal Plain Local Emergency Planning Committee (LEPC), and Corpus Christi-Nueces County LEPC. This engagement not only enhances interagency

communications but enhances overall port security by leveraging communication streams outside of traditional maritime networks.

6.0 Headquarters Input

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

Cybersecurity. Coast Guard Headquarters continues to develop guidance and other resources to address cyber safety, security, and cyber risk management within the MTS.

- The Coast Guard published a Notice of Proposed Rulemaking proposing to update its maritime security regulations by adding regulations specifically focused on establishing minimum cybersecurity requirements for U.S. flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to the MTSA regulations. This proposed rulemaking would help to address current and emerging cybersecurity threats in the marine transportation system.
- The Coast Guard published Navigation and Inspection Circular (NVIC) 02-24. On February 21, 2024, President Biden signed Executive Order 14116. Among other provisions, this Executive Order added a definition for "cyber incident" and created a requirement to report evidence of an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility to the Coast Guard, the Federal Bureau of Investigation (FBI), and CISA. The broad applicability of 33 CFR Part 6 and the new definition of a cyber incident created an overlap with existing MTSA reporting requirements. NVIC 02-24 provides clarification and voluntary guidance on the reporting requirements identified in 33 CFR Part 101 and 33 CFR Part 6.
- The Coast Guard issued Maritime Security (MARSEC) Directive 105-4, providing cyber risk management actions for owners or operators of ship-to-shore (STS) cranes manufactured by People's Republic of China (PRC) companies (PRC-manufactured STS cranes).
- The Coast Guard provided guidance for AMSCs to address cyber through NVIC 09-02 CH 6, which includes an Area Maritime Security Assessment and a template for a Cyber Incident Response Plan.
- The Coast Guard Auxiliary is actively working with key USCG partner organizations to formalize the establishment of an Auxiliary Cybersecurity Augmentation program (AUXCYBER). The program is being established to allow qualified Auxiliarists with a broad range of expertise in cybersecurity and cyberspace operations to augment the Coast Guard cyberspace workforce, including but not limited to cybersecurity outreach, awareness, education, training, and cyber exercise support.

UAS. The Coast Guard continued to receive reports in UAS sightings over or near maritime critical infrastructure in 2023.

- The Office of Maritime Security Response Policy (CG-MSR), in partnership with the Office of Specialized Capabilities (CG-721), manages the development and implementation efforts relating to C-UAS authorities, capabilities, and operational policies in support of CG missions. CG-721 can assist CG Units with C-UAS capability and training requests. CG-721 also engages with the CG Research and Development Center and with DHS Science and Technology Directorate C-UAS Program which assesses new technology to assist DHS components.
- CG-FAC continues to work with FAA on the National Proposed Rule Making to update Section 2209 of the FAA Extension, Safety, and Security Act. On May 9, 2024, the U.S. Senate approved the FAA Reauthorization Act of 2024 and on May 15, 2024, it passed the House of Representatives and was signed by the POTUS on May 16, 2024. Passing the act authorized the act to continue until FY2028. Also, NVIC 02-24, Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents (that would impact a MTSA regulated entity), includes a section that addresses unauthorized UAS activity and how to report. Additionally, FAA has a website that provides a geospatial display of all current UAS related airspace restrictions: Visualize it: See FAA UAS Data on a Map (arcgis.com)

AS/AT. The US Coast Guard and various other maritime security forces must ready themselves for potential attacks, whether targeting shoreside facilities or vessels underway such as ferries or dinner cruises and continue to conduct training sessions with local, state, and other governmental agencies in accordance with the Coast Guard training protocols.

- The Office of Maritime Security Response Policy (CG-MSR) Maritime Security Response Operations (MSRO) tool has recently introduced new competency codes (Instructor/Operator) aimed at identifying and establishing a standardized framework for the skills, knowledge, and abilities necessary to respond proficiently to active shooter incidents. This initiative ensures uniformity across training initiatives and enhances collaboration among various agencies and jurisdictions.
- In April 2024, CG-MSR participated in the Law Enforcement Coordination Council (LECC) held in Glynco, GA. The mission of the LECC program is to foster communication, coordination, and cooperation among state, local, and federal law enforcement agencies. The council assessed the DHS AS/AT curriculum for consistency, performed a gap analysis, and offered actionable recommendations.

MTS Resilience/Recovery. The 2023 hurricane season was the fourth most active hurricane season on record. In total, there were twenty named storms, with seven that developed into hurricanes. Four storms and their remnants made landfall in the contiguous U.S., with Idalia, a category-3 hurricane having impacted Florida and the southern states, being attributed to 12 fatalities and $3.6 billion in damages. Additionally, tropical storm Hillary, the first tropical storm

to hit southern California in 84 years, broke record rain falls, caused severe flooding, and led to extensive transportation disruptions. These storms, and all other 2023 storms, resulted in a combined $60 billion in damages across the U.S.

Emergency Support Function-1 watch standers worked quickly to consolidate information and communicated to senior leadership, enabling them to take necessary action to mitigate impacts to the MTS. Overcoming these challenges were the result of outstanding work by local MTS Recovery Units and communication between all levels of command. Senior leaders in FEMA, the 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, state, local, tribal, and territorial officials, and our industry port partners to support MTS safety, security, and resilience.

7.0 Conclusion

The MTS remains at the forefront of national security and economic interests. AMSCs are an essential part of the maritime security regime and must continue to evolve and adapt accordingly to combat emerging threats while ensuring the unimpeded flow of commerce. Security challenges, whether physical or cyber related, remain a constant fixture and continue to pose potential adverse impacts to our critical ports and waterways. Continued collaboration, information sharing, and coordination via AMSCs are vital to mitigating risks and crucial to the efficient facilitation of commerce.