Area Maritime Security Committees

Challenges, Suggestions, Accomplishments, and Best Practices

2017 Annual Report

U.S. Coast Guard

Washington, D.C.

Contents

- **Introduction**
  - *1.0 – Background*
  - *2.0 – Challenges*
  - *3.0 – Suggestions*
  - *4.0 – Accomplishments*
  - *5.0 – Best Practices*
  - *6.0 – CG Headquarters Input*
  - *7.0 - Conclusion*
- **Online Enclosures**
  - *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 Chief's Perspective

How we secure our ports substantially changed with the implementation of the Maritime Transportation Security Act (MTSA) of 2002. This act specifically authorized the establishment of Area Maritime Security Committees (AMSCs). Currently there are 43 AMSCs established around the country to include Guam/Northern Mariana Islands, Hawaii/American Samoa, Puerto Rico/U.S. Virgin Islands, and Alaska (Anchorage, Juneau, and Valdez). Each AMSC is led by the local U.S. Coast Guard Captain of the Port (COTP)/Federal Maritime Security Coordinator (FMSC) and provides a valuable forum to discuss and address maritime security issues at the port level. AMSCs are comprised of subject matter experts from Federal, Territorial, Tribal, State, and Local agencies as well as public and private port stakeholders to ensure the safety, security, and resilience of our nation's critical Marine Transportation System (MTS).

The MTS is comprised of over 25,000 miles of commercially navigable waterways, 361 ports, and more than 3,700 marine terminals. 90% of imports and exports enter or leave the United States by vessel. Additionally, MTS activities contribute more than $4.6 trillion dollars of economic activity, sustaining more than 23 million jobs. Through effective coordination, collaborative planning, open communications, and strong working relationships, AMSCs have proven their value to bolstering the safety and security of the MTS.

Looking ahead, we face dynamic challenges in the global maritime spectrum. AMSCs will remain essential to addressing evolving issues such as cybersecurity, domestic energy transportation, and other emerging issues and threats. This Annual Report highlights the many achievements of the AMSCs and serves as a reminder of all the outstanding work and efforts performed by port partners/stakeholders as well as Coast Guard men and women.

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

1.0 Background

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

2.0 Challenges

AMSCs identified specific challenges or impediments they encountered in 2017. Enclosure (1) identifies all challenges reported from each AMSC in 2017. The following highlight common challenges:

Cyber Security and the Marine Transportation System (MTS). As noted in the 2016 annual report, cyber security in the MTS continued to be a challenge in 2017. In June, a global shipping company's information technology (IT) systems (phones, emails, communications, etc.) were adversely impacted by a malware virus. Although the virus did not affect operational technology (OT) systems of terminals or vessels (security systems, environmental systems, navigational systems, etc.), the results of the IT intrusion were significant causing the shipping company to shut down all of its IT systems which considerably slowed operations at 76 terminals worldwide, including five major terminals in the United States. This incident was a clear reminder of the importance of cyber risk management in the MTS both nationally and globally. The rapid progression of software development and the technical aspects of thwarting cyber-incidents or attacks presents serious constraints to the maritime industry and Coast Guard personnel who have limited knowledge of computer systems and cyber technology. The dynamic nature of cyber security threats and the shortage of subject matter experts make cyber security preparedness and response a continuing challenge.

Homeport upgrade to Homeport 2.0. Homeport is the United States Coast Guard's enterprise Internet portal. It was designed to support the secure information sharing requirements described in the Maritime Transportation Security Act of 2002 (MTSA). Homeport allows the ability to bring together Coast Guard personnel, members of the maritime community, and other designated individuals to share information quickly. The upgrade to Homeport 2.0 was identified as a challenge for the AMSC community. A new user guide for Homeport 2.0 lacked necessary details making it difficult for local Homeport administrators to set up certain information sharing communities. In addition, some features of Homeport 2.0, such as AMSC management tools were not functional. Furthermore, industry and other government users were required to work through a National Help Desk to address Homeport 2.0 concerns, eliminating the previous ability of users to directly reach out to local Homeport administrators

at the port level. This new process lengthened response times and hindered the use and effectiveness of Homeport 2.0.

Unmanned Aerial Systems (UAS) access to the MTS. UASs continued to be a major concern for the safety and security of the maritime community. The ability of a UAS to circumvent access control measures poses significant challenges. Reported incidents of UASs operated in close proximity to commercial vessels and waterfront facilities were more prevalent in 2017 and in some reported cases, were operated dangerously close to vessels underway. Law enforcement at all levels of government lack uniform regulations, policy, techniques, tactics, procedures, and equipment needed to safely interdict and prosecute cases where maritime infrastructure and key assets are exposed to potential risks posed by UASs.

Port Security Specialist (PSS) expansive responsibilities. Responsibility for managing the AMSC and maintaining the Area Maritime Security Plan (AMSP) falls primarily on Coast Guard civilian PSS. Other PSS responsibilities include managing the Maritime Security Risk Analysis Model (MSRAM), overseeing Port Security Grant Program (PSGP) applications, administration of the Area Maritime Security Training and Exercise Program (AMSTEP), management of Homeport 2.0 and the port partner Alert Warning System (AWS) as well as salvage and port recovery planning. All these responsibilities plus new, evolving risks to the MTS such as cybersecurity are stressing this limited workforce.

Public Access Facilities safety and security. Various open sources continued to highlight the threat posed by individuals who use tactics and weapons such as improvised explosive devices, vehicle ramming, small arms, and edged weapons at large public gatherings. Attacks perpetrated by individuals using the above noted tactics, particularly in places where crowds gather is a significant concern. In such an event, the response time alone could exacerbate an incident. AMSCs are an exceptional touch point for building capabilities and partnerships within the port to help mitigate, deter, or prevent such incidents.

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 2017:

Cyber Security/Cyber Risk Management. Field units request more guidance/policy from CG Headquarters relating to cyber security issues in the maritime domain as well as developing training on preparedness, resiliency, and recovery from a cyber security incident. Many AMSCs recommend open dialogue and engagement with the Federal Bureau of Investigation's (FBI) InfraGard program as another effective information sharing resource.

Homeport 2.0. A new, upgraded version of Homeport was introduced in the fall of 2017. Section 2.0 of this report noted the numerous challenges faced by this upgrade. One of the prevalent suggestions indicated by AMSCs was the need for additional training for field level users and administrators.

Unmanned Aerial Systems (UAS). AMSCs recommend the U.S. Coast Guard (USCG) and Department of Homeland Security (DHS) support any legislative and/or policy efforts to provide Federal, State and Local law enforcement with authorities to identify, interdict, and ultimately prosecute cases where maritime infrastructure and key assets of the MTS are at risk from UASs. Additionally, the USCG and DHS should support the creation of techniques, tactics, procedures, and funding for equipment needed to address potential risks associated with nefarious or negligent use of UASs.

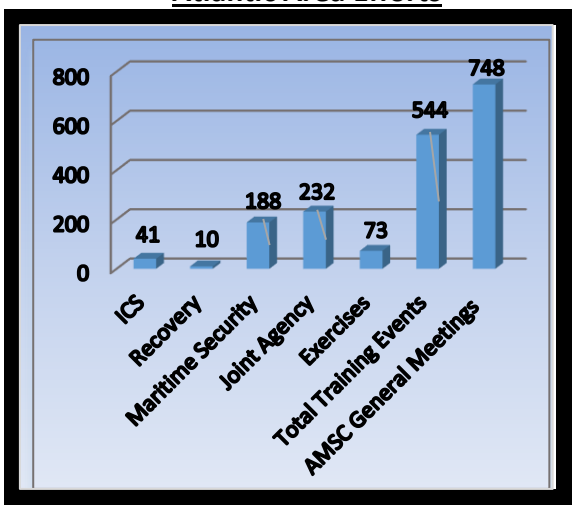
Active Shooter incidents: AMSCs have facilitated active shooter workshops and other training for relevant subcommittees (e.g., law enforcement, intelligence, etc.). Many AMSCs recommend port partners incorporate active shooter scenarios into their safety and security drills.

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 2017, AMSCs and their respective subcommittees collectively facilitated 1,857 events. This total included 950 administrative AMSC meetings (e.g., Executive Steering Committees and General AMSC meetings) and 624 training specific events (includes 245 Joint Agency training meetings, 201 maritime security training operations, 82 training exercises, 81 Incident Command System and 15 MTS Recovery Unit training sessions). These coordinated opportunities resulted in effective, real world security prevention, response, and recovery efforts. Enclosure (3) identifies accomplishments reported from each AMSC in 2017.

The following tables highlight AMSC efforts nationwide.

Atlantic Area Efforts



Pacific Area Efforts

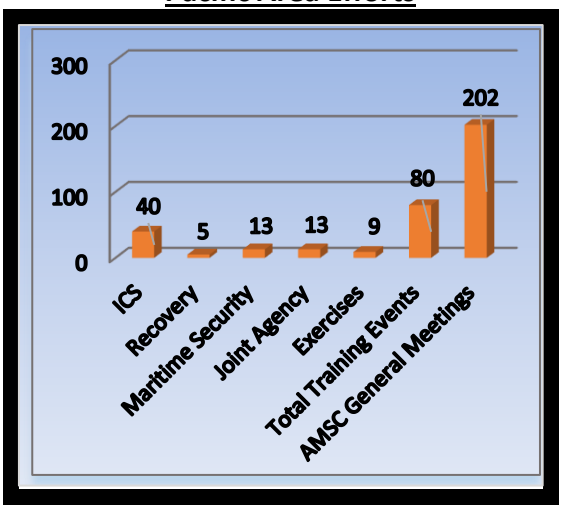


Figure 1 - AMSC Nationwide training break down by Areas: ICS includes FEMA and Emergency Response incident command training; Recovery includes MTSRU training; Maritime Security includes MSRAM, Cyber, TWIC, and Port Ops training; Joint Agency includes all interaction with federal, state, local partners/stakeholders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

Cyber: AMSCs continued to engage in multiple cyber security related activities. Currently 29 AMSCs have established cyber security subcommittees to assist in addressing cyber risk, information sharing, and ways to enhance preparedness/resilience of cyber-related incidents. AMSCs that have not established a specific cyber subcommittee address cyber issues in other well established subcommittees (e.g., Intel, Law Enforcement, etc.). The following are examples of AMSC cyber activities. The Long Island Sound AMSC and Northern California AMSC participated in the 2017 National Cyber Guard Prelude exercise. The New York and New Jersey AMSC held multiple cyber related meetings, workshops, exercises, and drafted AMSC guidance to address cyber security in its area of operation. The Sault Region AMSC established a partnership with Michigan's Department of Technology Management and Budget for cybersecurity-related issues/training.

Active Shooter: AMSCs addressed ways to mitigate physical threats in the marine environment. As examples, the New York and New Jersey AMSC's Response and Recovery subcommittee determined a waterborne active shooter incident was a threat they must address. As a result, the AMSC's small passenger vessel subcommittee assisted with the collection of risk analysis data related to such an incident to develop response protocols and draft a Passenger Ferry Active Threat Plan. COTPs/FMSCs all over the country conducted multiple workshops and other exercises in conjunction with AMSCs for the purpose of defining roles, responsibilities, and drafting concepts of operations to assist AMSCs with various physical threats.

Preventive Radiological and Nuclear Detection (PRND): PRND Initiatives sponsored by the Domestic Nuclear Detection Office (DNDO) continued to be a focal point for AMSCs. The Charleston AMSC responded to a real world "dirty bomb" report involving an inbound foreign flagged container ship. The Charleston AMSC implemented its Area Maritime Security Plan's Radiological/Nuclear (RAD/NUC) detection and response annex that led to joint operational planning and information sharing amongst AMSC members fostering quick and effective deployment of assets to resolve the concern and protect public safety. Based on the successful implementation of the AMSP RAD/NUC annex, the Charleston AMSC's RAD/NUC subcommittee shared its plan with numerous AMSCs across the country.

RAD/NUC CONOPS. The Paducah AMSC completed the process of identifying agencies, developing CONOPs and standard operating procedures, training personnel, and deploying detection equipment in support of the preventive RAD/NUC mission for the Western Rivers. The AMSC and members of Marine Safety Unit Paducah worked directly with representatives from the DNDO and Oak Ridge National Laboratory to accomplish this task. The Southeastern New England AMSC held a workshop to present the contents of its recently developed PRND Concept of Operations (CONOPs). The Ohio Valley AMSC held multiple RAD/NUC training events.

Exemplary Work by a Communication Subcommittee. The Charleston AMSC Communications subcommittee leveraged its membership to augment an existing Common Operating Picture (COP) resource known as ALASTAR used by the local county dispatch and the 911 call-center to provide increased coverage of the MTS. The subcommittee identified and solicited maritime stakeholders to share remote technologies with ALASTAR resulting in the expansion of the system's capabilities by providing real-time and on-demand video coverage for an additional 30% of the waterways in the local COTP zone.

Ferry Boat Security Training Course Development. The Southeastern New England AMSC was an integral partner with the Coast Guard's Research and Development Center to address a Department of Homeland Security's Science and Technology (DHS S&T) Directorate initiative to develop a prototype Ferry Boat Security Training course. The course was developed based on industry responses to the 2016 National Census of Ferry Operators with the intent to enhance awareness and resiliency of front-line ferry boat personnel. The voluntary training course includes four modules (1) Understanding the Terrorism Landscape, (2) Reducing Vulnerabilities (3) Suspicious Activities - Behaviors and Objects, and (4) Incident Reporting. DHS S&T anticipates the course will be completed by October 31, 2018 and will be made available to the public.

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 2017.

Homeland Security Information Network (HSIN) and AMSC Meetings. The Long Island Sound (LIS) AMSC continued to successfully use HSIN Adobe Connect to hold virtual AMSC Executive Steering Committee (ESC) and subcommittee meetings. This has resulted in reduced travel costs, allowed members spread out over a large geographical area the ability to actively engage in the AMSC, and provided the AMSC ESC a "virtual" alternative to facilitate information sharing among members. HSIN Adobe Connect virtual meeting rooms are maintained by the executive secretary for the AMSC and for the three Connecticut regional port area Marine Group subcommittees (An example can be found at: https://share.dhs.gov/amsc-esc/).

Additionally, HSIN Adobe Connect provides a link to a free mobile smart phone app at http://www.adobe.com/products/adobeconnect/mobile-meetings.html. This app allows partners to use smart phones to participate in HSIN Adobe Connect meetings and includes the ability to stream and view videos/pictures. The LIS AMSC highly recommends all AMSCs establish a Community of Interest in HSIN to assist with virtual meetings and information sharing. For more information on HSIN contact their outreach team at HSIN.Outreach@hq.dhs.gov or visit https://www.dhs.gov/homeland-security-information-network-hsin

Maritime Tactical Operations Working Group Creation: The Delaware Bay AMSC identified the need for a forum that could focus on maritime tactical operations, the AMSC surveyed other AMSCs nationwide and requested information on Law Enforcement or Special Operations sub-committees. Based on models and best practices from other AMSCs, Delaware Bay's AMSC stood-up a Maritime Tactical Operations Working Group (MTOG). Since its conception, the MTOG has enhanced innovation and improved communications among law enforcement and fire departments within the COTP zone. The relationships built through the MTOG made a positive impact in exercise participation and coordinated responses to real time events.

Testing of Newly Developed RAD/NUC CONOPs. The Port of Huntington/Tri-State AMSC participated in its first ever, RAD/NUC Tabletop and Full-Scale Exercise hosted by the Cabell and Wayne County, West Virginia Local Emergency Planning Committee (LEPC). The exercise series was the first to test the AMSC's newly developed RAD/NUC CONOPs. Lessons learned from the exercises will guide future development of response programs, equipment procurement, and training initiatives in the port.

Unmanned Aerial Systems (UAS). Various AMSCs have held discussions regarding UASs. Port partners have been educated on federal and state regulations governing UAS usage and potential actions available. In most ports, AMSC port partners send out notifications when a legitimate UAS is utilized near critical maritime infrastructure. One AMSC has formed a working group with their regional Federal Aviation Administration (FAA) office.

Survey of AMSC members. The Puget Sound AMSC sponsored a survey of all AMSC members. The goal of the survey was to determine if AMSC agendas were meeting the expectations of membership. The results of the survey led to three primary recommended changes: (1) remove presentations or presenters related to the sale of commercial products, (2) publish a year-long meeting calendar, and (3) rotate the general AMSC meeting to other venues within Puget Sound.

Cyber Range use. The Hawaii and American Samoa AMSC used the unique capabilities of the University of Hawaii's Cyber Range to combine a functional, information technology (IT)-based exercise with a traditional discussion-based tabletop exercise to address maritime cyber threats. The exercise brought IT managers and technical staff together with corporate leadership, maritime operations personnel, and government agencies. This fusion of disciplines highlighted the challenges faced when translating technical cybersecurity concepts to less tech-savvy decision-makers and illustrated the complexities of building secure network environments for maritime critical infrastructure. Additionally, the exercise raised awareness of the threat of cyber-attacks on the MTS and exposed port partners to potential real-world consequences of such an attack. As a result, the AMSC subsequently partnered with the FBI's InfraGard program to charter a joint maritime Special Interest Group (SIG)/AMSC cybersecurity workgroup. Recognizing cyber-threats are not exclusive to the maritime domain, the SIG will

provide an ongoing opportunity for port security stakeholders to network and share information with colleagues from other critical infrastructure sectors and industries.

Maritime Domain Awareness and Common Operating Picture. Many companies offer off the shelf solutions to assist in combining and sharing real-time data to increase and improve Maritime Domain Awareness. The Charleston AMSC incorporated one such solution called ALASTAR. According to the manufacture, ALASTAR provides public safety personnel access to a comprehensive, dynamic, real-time, portable view of regional activities, and the capability to conduct interagency collaboration across multiple jurisdictions and discipline. AMSC members achieved consensus agreement to cost-share the tool enabling equal access by all AMSC members, and, through a joint Port Security Grant application, AMSC agencies and organizations will have the means to fund the use of ALASTAR in 2018. Quarterly training and software development sessions hosted by the AMSC's communications subcommittee provided end-users opportunities to heighten their knowledge of the system and provided ALASTAR software engineers needed user feedback to tailor, design, and implement system enhancements. The Charleston AMSC's use of ALASTAR has been a resounding success.

6.0 CG Headquarters Input

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

Cyber. Cyber-related risks are a growing portion of the vulnerabilities facing the MTS. Cyber technologies enable the MTS to operate with an impressive record of reliability and at a capacity that drives the U.S. economy and supports national defense, homeland security, and related needs. While cyber systems create benefits, they also introduce risk. Exploitation, misuse, or failure of cyber systems could cause harm to the marine environment or disrupt vital trade activity. Even a temporary or partial disruption of MTS operations could have serious consequences. As a result, cyber risk management has become increasingly important. COTPs/FMSCs should continue to leverage engagement via AMSCs and cyber subcommittees.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework was developed in 2014 to address and manage cybersecurity risk in a cost-effective way based on business needs and without placing additional regulatory requirements on businesses. Because of the coordination between the Coast Guard Office of Port and Facility Compliance (CG-FAC), the NIST's National Cybersecurity Center of Excellence (NCCoE), key industry stakeholders, and trade associations, two cybersecurity framework profiles (CFPs) were developed in 2017. The Offshore Operations and the Passenger Vessel industry profiles reflect how organizations align the NIST framework's cybersecurity activities, outcomes, and informative references to organizational business requirements, risk tolerances, and resources. The CFPs outline a desired minimum state of cybersecurity and cyber risk management, and provide the opportunity to plan for future business decisions. The CFPs were published in January 2018 and follow the November 2016 release of the Maritime Bulk Liquid Transfer CFP. All CFPs are voluntary cyber risk assessment tools and are the first of their kind for the Marine Transportation System

sector. The Coast Guard anticipates working with the NCCoE on at least one additional profile addressing navigational systems and facility automation.

In late 2017, the Office of Cyberspace Forces (CG-791) was stood up at Coast Guard Headquarters to implement the Coast Guard Cyber Strategy and manage the Cyber Program. CG-791 delivers programmatic oversight and direction for the organization, training, equipping, and operational policy for the cyberspace workforce, and develops strategy and policy for enabling operations and protecting the Marine Transportation System (MTS) infrastructure. CG-791 falls under the purview of the Assistant Commandant for Capability (CG-7) and collaborates with various Prevention Policy offices (CG-5P), including CG-FAC, to support the "Protecting Infrastructure" priority of the Coast Guard's Cyber Strategy.

*Unmanned Aerial System (UAS)***.** In September 2017 at a U.S. Senate hearing, the FBI Director announced that the use of UASs to carry out terrorist attacks is an imminent threat to the Homeland. At the same hearing, the Director of the National Counter Terrorism Center (NCTC) stated that terrorist groups are utilizing weaponized UASs overseas. As a result, concerns were raised on the illicit use of UASs stateside. The Coast Guard reminds MTSA regulated entities that UAS suspicious activities and breaches of security reporting requirements can be found in CG-5P Policy Letter 08-16 dated December 14, 2016 and titled "Reporting Suspicious Activity and Breaches of Security."

Within the maritime community, port partners have incorporated UASs as a cost effective tool for various operations such as safety inspections, emergency response monitoring, and other legitimate actions. Most states (41) have enacted laws addressing UASs and an additional three states have adopted resolutions. AMSCs are recommending further changes/modification of the current federal UAS legislation and to provide state and local law enforcement entities the additional authorities to identify, interdict, and prosecute cases where maritime infrastructure and key assets are at risk from UASs. FAA has formed a Law Enforcement Working Group to discuss and track concerns with UASs.

Policy Advisory Council (PAC) Document Registry. The PAC Document Registry is a collection of PAC decision documents (PACs) that provide the intent of certain regulations covered under MTSA. PACs are a valuable tool for understanding various maritime security regulations that impact AMSC and maritime industry equities. PACs began in 2003 with with the last PAC published in March of 2011. Revisions and cancellations of PACs over the years have caused confusion. As a result, CG-FAC completed a comprehensive review of all PACs in 2017. The new registry of current PACs is available at https://homeport.uscg.mil/missions/maritime-security/maritime-transportation-security-act-(mtsa)/faqs or please contact the local AMSC executive secretary for additional information.

Marine Transportation System (MTS) Resilience/Recovery. The 2017 Hurricane season was one of the most devastating seasons on record. Hurricanes Harvey, Irma and Maria required maritime stakeholders from Texas, Florida, Puerto Rico and the Virgin Islands to prepare for and respond to a MTS disruption along the Gulf Coast, Southeast Coast, and Caribbean Islands.

National planning for these hurricanes included identifying Coast Guard PSSs and Security Specialists (Port Recovery) from outside the impacted areas to prepare for deployment in support of MTS Recovery operations at affected units and coordinating with Customs and Border Protection and Department of Transportation personnel managing the FEMA Emergency Support Function One response. Coast Guard lead MTS Recovery Units at the Area, District, and Sector level which included participation from other Federal, Territorial, Tribal, State, Local, Private and Public port stake holders were integral to effective short-term recovery and resumption of commercial maritime operations to those impacted areas.

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 waterways. Continued collaboration, information sharing, and coordination via AMSCs are vital to mitigating risks and crucial to the efficient facilitation of commerce.