# The Maritime Security Center (MSC)

at Stevens Institute of Technology

Hoboken, NJ

# Annual Report

Year 7

July 1, 2020 through June 30, 2021

January 2022

# TABLE OF CONTENTS


**1 BACKGROUND ..... 4**

**2 RESEARCH PROJECTS ..... 4**

2.1 Low-Cost Covert Sensors for Remote Locations Project ..... 4
*2.1.1 Abstract ..... 4*
*2.1.2 Changes from Initial Workplan ..... 6*
*2.1.3 Objective ..... 7*
*2.1.4 Baseline ..... 10*
*2.1.5 Methodology ..... 11*
*2.1.6 Milestones and Performance Metrics ..... 17*
*2.1.7 Transition Considerations ..... 19*
*2.1.8 Stakeholder Engagement ..... 22*
*2.1.9 Potential Programmatic Risks ..... 23*
*2.1.10 Progress Against Milestone Outcomes ..... 23*
*2.1.11 Unanticipated Problems ..... 23*
*2.1.12 Information Supported by Data ..... 23*
2.2 RF Surveillance Project ..... 25
*2.2.1 Abstract ..... 25*
*2.2.2 Changes from Initial Workplan ..... 26*
*2.2.3 Objective ..... 27*
*2.2.4 Baseline ..... 36*
*2.2.5 Methodology ..... 37*
*2.2.6 Project Milestones and Performance Metrics ..... 38*
*2.2.7 Transition Plan ..... 44*
*2.2.8 Stakeholder Engagement ..... 45*
*2.2.9 Programmatic Risks ..... 46*
*2.2.10 Progress ..... 46*
*2.2.11 Unanticipated Problems ..... 46*
*2.2.12 Information supported by data ..... 46*
2.3 Safety and Security of Remote Bridge Operations Project ..... 47
*2.3.1 Changes from Initial Work Plan ..... 47*
*2.3.2 Objective ..... 47*
*2.3.3 Baseline ..... 48*
*2.3.4 Methodology ..... 48*
*2.3.5 Milestones and Performance Metrics ..... 49*
*2.3.6 Transition Considerations ..... 50*
*2.3.7 Stakeholder Engagement ..... 50*
*2.3.8 Potential Programmatic Risks ..... 52*
*2.3.9 Unanticipated Problems ..... 52*
*2.3.10 Information Supported by Data ..... 53*
2.4 VTS Radar for Small Vessel Detection ..... 53
*2.4.1 Changes from Initial Workplan ..... 53*
*2.4.2 Objective ..... 53*
*2.4.3 Baseline ..... 54*
*2.4.4 Methodology ..... 55*
*2.4.5 Project Milestones and Performance Metrics ..... 59*
*2.4.6 Transition Considerations ..... 60*
*2.4.7 Stakeholder Engagement ..... 60*
*2.4.8 Potential Programmatic Risks ..... 62*
*2.4.9 Progress Against Milestone Outcomes ..... 62*
*2.4.10 Unanticipated Problems ..... 62*
*2.4.11 Information Supported by Data ..... 62*

**3 EDUCATION AND OUTREACH ..... 69**

3.1 Summary of Education Milestones ..... 69

*3.1.1 Summer Research Institute (SRI)* ... *69*
*3.1.2 Undergraduate and Graduate-level Research Assistantships* ... *70*
*3.1.3 MSI STEM Educator's Workshop* ... *70*
*3.1.4 MSI Summer Research Team Program* ... *70*
*3.1.5 Maritime Cybersecurity Professional Development Pilot Course* ... *70*
3.2 THE SUMMER RESEARCH INSTITUTE (SRI) ... 71
*3.2.1 Milestones and Performance Metrics* ... *71*
*3.2.2 Overview* ... *72*
*3.2.3 Student Qualifications and Documentation* ... *74*
*3.2.4 Summer Research Stipends* ... *74*
*3.2.5 Program Administration* ... *74*
*3.2.6 Program Format and Curriculum* ... *74*
*3.2.7 Meetings with Homeland Security Professionals* ... *78*
*3.2.8 Student Research Projects* ... *79*
*3.2.9 SRI 2021 Student Survey* ... *92*
3.3 GRADUATE AND UNDERGRADUATE RESEARCH ASSISTANTSHIP PROGRAMS ... 94
*3.3.1 Milestones and Metrics* ... *94*
*3.3.2 MSC Research Students* ... *95*
*3.3.3 Graduate Research Assistants* ... *96*
*3.3.4 Undergraduate Research Assistants* ... *98*
3.4 MSI ENGAGEMENT WORKSHOP ... 98
*3.4.1 Milestones and Performance Metrics* ... *98*
*3.4.2 MSI Workshop* ... *99*
3.5 DHS MSI SUMMER RESEARCH TEAM ... 101
3.6 MARITIME CYBERSECURITY PROFESSIONAL DEVELOPMENT COURSE ... 102
*3.6.1 Overview and Objectives* ... *102*
*3.6.2 Project Milestones and Performance Metrics* ... *102*
*3.6.3 Maritime Cybersecurity Professional Development Pilot Course – Planning and Delivery* ... *104*
*3.6.4 Course Modules and Delivery Format* ... *105*
*3.6.5 LANTAREA Pilot Course Feedback* ... *106*
*3.6.6 PACAREA Pilot Course Feedback* ... *107*
*3.6.7 Ongoing Course Delivery* ... *108*

**4 COMMUNICATIONS AND OUTREACH ... 109**

**5 OTHER RELATED ACTIVITIES ... 109**

5.1 PROJECT SOLICITATION ... 109
5.2 STAKEHOLDER ENGAGEMENT, COMMUNICATIONS, AND OUTREACH ... 110
5.3 OTHER ACTIVITIES ... 112
5.4 MANAGEMENT ACTIVITIES ... 112
5.5 CENTER GUIDELINES AND POLICIES ... 113

**6 BUDGET ... 113**

**APPENDIX E-1 SRI 2020 STUDENT SURVEY ... 115**

**APPENDIX E-2 MARITIME TRANSPORTATION CYBERSECURITY MSI WORKSHOP SURVEY ... 119**

# 1 Background

The Maritime Security Center (MSC), a Department of Homeland Security (DHS) Science and Technology (S&T) National Center of Excellence (COE) was established in 2014 as a result of a competition conducted by DHS's Office of University Programs (OUP). MSC is led by Stevens Institute of Technology and this report is based on activities that were conducted by the MSC at Stevens under the Cooperative Agreement during Year 7 (July 1, 2020 through June 30, 2021).

MSC is composed of a consortium of internationally recognized research universities, including Stevens, Rutgers University, University of Illinois at Urbana-Champaign (lead university for the Critical Infrastructure Resilience Institute Center of Excellence), MIT, the University of Miami, the University of Puerto Rico, Louisiana State University, Florida Atlantic University, Purdue University, and Elizabeth City State University as well as industry partners, including the American Bureau of Shipping (ABS). The contributions of each partner institution during the reporting period are provided with the corresponding projects in this report.

MSC's mission is to develop both fundamental and applied research to support DHS's and other agencies' maritime security mission goals, including improved detection and interdiction capabilities, enhanced capacity to respond to catastrophic events, and a more secure and efficient Marine Transportation System (MTS). MSC has been focusing on interdisciplinary DHS mission-driven research, education, and technology transition in maritime security, maritime domain awareness, and resiliency issues. Our goal is to develop and transition research and technology solutions and educational programs to DHS maritime stakeholders, such as the US Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and other related agencies and to improve capabilities and capacities for preventing and responding to events in the maritime domain. The next section describes the research projects.

# 2 Research Projects

This section discusses the Low-Cost Covert Sensors for Remote Locations, RF Surveillance, Safety and Security of Remote Bridge Operations, and VTS Radar for Small Vessel Detection research projects. These projects were in the work plan that was approved for Year 7.

## 2.1 Low-Cost Covert Sensors for Remote Locations Project

PI: Dr. Alexander Sutin, Stevens Institute of Technology
Project Period: September 2019 - June 2021
Budget: $494,514

### 2.1.1 Abstract

Detection of small boats, semisubmersibles, and underwater vehicles is required for several USCG missions, including drug and alien migrant interdiction, monitoring, control,

and surveillance of illegal, unregulated, and unreported (IUU) fishing, as well as protection from maritime terrorist activity. The USCG uses numerous sensors installed on land, cutters, aircraft, helicopters, unmanned aircraft systems (UAS), and satellites that detect vessels involving illegal activity. Significant improvement of UCSG performance and decrease of operational costs may benefit from using low-cost, unmanned, maritime domain awareness technologies and sensors that can monitor remote locations covertly and provide actionable information. As described in the Maritime Security Center's Year *7* Work Plan, the goal of this project was to build and test a low-cost sensor suite for the detection of illegal vessel traffic.

Several experimental sensor suites were built and tested that use low-cost COTS sensors including marine radars, optical and infrared cameras, and AIS receivers in conjunction with an underwater acoustic array, the **S**tevens **P***a*ssive **A**coustics ***DE****tection* **S**ystem (SPADES), outfitted with low-cost hydrophones. The Boat Detection System (BDS) developed through this project, can work autonomously at sea and may be deployed on available platforms such as oil rigs, navigation and communication buoys. The BDS can be installed on remote shore locations or on land-based communication and security towers. BDS uses its data fusion algorithm to generate and send alerts and reports to a USCG Sector Command for illegal traffic interdiction.

The simplest and lowest cost sensor suite consists of radar, camera and AIS receiver with proprietary software for automated boat detection and tracking. The total component cost of this simplified system (BDS1) is under $6,000 and can provide automated alerts to USCG about nefarious boat presence. The full system (BDS2) includes an acoustic sensor (SPADES) that extends the detection range especially of Targets of Interest (ToI) with a low radar cross-section (RCS), semi submersibles, and other low-profile vessels. The component cost of a single SPADES node is about $11,000, which leads to a total component cost of $17,000 for the BDS2 system.

Several iterations of BDS with different sensors were investigated. In January of 2020, the first test was conducted in the Padre Island area of Texas in the Area of Responsibility of the USCG Sector Corpus Christi. The shore-based setup provided the information needed to develop an appropriate sensor suite for the area and whether the result would be shore or off-shore based. This test demonstrated that the acoustic sensor could detect a small boat at much farther distances than the radar. The acoustic detection distance of a small boat in the shallow sea in the Padre Island was about 8 km.

A variety of sensors were tested during deployment of BDS on the Hudson River over the course of several months, including three different radars and an IR FLIR camera. The best BDS performance was reached using a Simrad Halo 24 radar. The IR camera provides much lower resolution than the optical camera, however, the price of the IR camera is about 10 times higher, so IR is less suitable for applications requiring a low-cost boat detection system. Radar and acoustic sensors provide ToI detection night and day. Additional information for ToI classification may also be extracted from acoustic signatures.

The tests conducted resulted in a collection of a large library of acoustic, radar, and optical vessel signatures. Acoustic signatures can also be used for vessel classification,

identification, and for finding the specifics of a boat's activity. For example, acoustics can detect fishing vessels performing trawling. Long-term test result analyses were used to measure the performance of BDS.

### 2.1.2 Changes from Initial Workplan

The goal of this project was to build and test a low-cost sensor suite for the detection of illegal vessel traffic. The low-cost sensor suite that was developed consists of a marine radar, an underwater acoustic system prototype, optical/IR cameras, and AIS receivers. The developed Boat Detection System (BDS) can work autonomously at sea and may be deployed on available platforms such as oil rigs and navigation and communication buoys. The BDS can be installed on remote shore locations as well, or on land-based communication and security towers.

At the beginning of the project (during September 2019 to July 2020), the work was progressing ahead of schedule. The first test was conducted in January 2020 in the Padre Island geographical area in Texas, located in the USCG Sector Corpus Christi Area of Responsibility (AOR). The original plan was for the installation of a prototype sensor suite with recording capability at an oil rig in the Padre Island area, however, due to logistical delays with the offshore wellheads and oil rigs in the area, a shore-based setup was deployed instead. The shore-based setup effectively provided the information needed for the development of the sensor suite appropriate for this area.

Due to the COVID-19 pandemic, travel was restricted so the field tests at the USCG Sector Corpus Christi AOR were not possible. In addition, employers closed and asked employees to work from their homes. In order to continue to work on the project within the restrictions, the Stevens Institute of Technology research team decided to continue testing in the Hudson River, adjacent to the Stevens campus in Hoboken, NJ. The low-cost sensor suite was installed on the Stevens campus, on the sixth floor of a riverfront building in June 2020. The Babbio Center building has a patio that provides a clear view to vessel traffic on the Hudson River. The setup allowed radar, optical, and IR detection of various boats on the Hudson River under various environmental conditions.

The building of the acoustic system prototype (the Stevens Passive Acoustic DEtection System or SPADES-2) moved slower than was planned and the system was assembled and deployed in the Hudson River in March 2021. The system collected acoustic ship information for 3 months and was left operating after the end of the to collect additional data that may be useful for future work.

The research team's easy access to the Hudson River test site allowed extension of the initial work plan, including testing of additional sensors and extended the collection of a library of acoustic, radar, and optical vessel signatures. A variety of sensors were tested during the deployment of BDS on the Hudson River over the course of several months, including three different radars and an IR FLIR camera. The best BDS performance was reached using a Simrad Halo 24 radar. The IR camera provides much lower resolution than the optical camera, but the price of the IR camera is about 10 times higher, so IR is less suitable for applications requiring a low-cost boat detection system.

The data collected was used in the development of an automated target detection and fusion algorithm and software for providing law enforcement alerts and contact report.

### 2.1.3 Objective

Detection of small boats, semisubmersibles, and underwater vehicles is required for several USCG missions, including drug and illegal migrant interdiction, monitoring, control, and surveillance of illegal, unregulated, and unreported (IUU) fishing, as well as protection from maritime terrorist activity. Detection and monitoring of vessels involving illegal activity occurs principally through the collection, analysis, and dissemination of tactical information and strategic intelligence combined with effective sensors operating from land, air, and surface assets.

The USCG sought low-cost, unmanned, maritime domain awareness technologies and sensors that can monitor remote locations covertly and provide actionable information. Stevens built and tested a low-cost sensor suite prototype that can work autonomously at sea using available platforms. The suggested low-cost automated sensor system costs several orders of magnitude less than current land and air-based sensors and does not require a human in the loop for its operation.

The proposed experimental sensor suite used low-cost COTS sensors including a marine radar, optical and infrared cameras, and AIS receivers in conjunction with an underwater acoustic array, the Stevens Passive Acoustic System (SPADES) prototype, outfitted with Stevens made low-cost hydrophones.

A diagram of this system is presented in Figure 1.

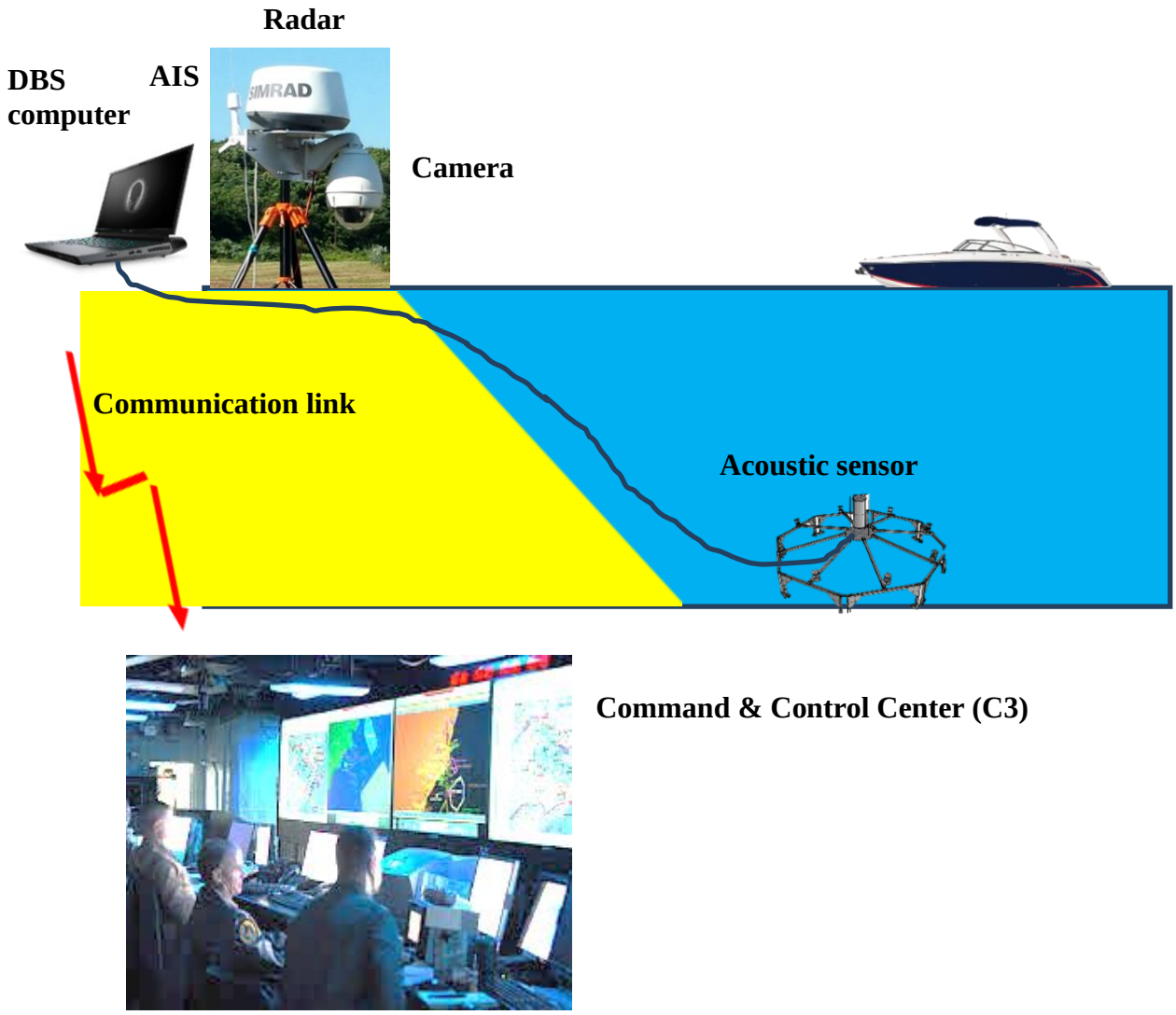



*Figure 1. Sketch of the Stevens Boat Detection System (BDS).*

Radars and optical/IR cameras are widely used for illegal boat detection. The goal of the work is to choose low-cost sensors and develop software for sensor data integration and USCG alert when suspected targets are detected.

The advantage of the suggested system is the implementation of acoustic sensors that enable reliable detection of small boats at night and in fog conditions. Acoustic sensors have longer coverage than low-cost radars and allow for the detection of Low-Profile Vessels (LPV) and Self-Propelled Semi-Submersibles (SPSS). LPV and SPSS produce strong underwater noise. Stevens has conducted field tests that have demonstrated that SPADES can detect SPSS at large distances (up to 40 km).

Acoustic sensors can provide additional information about boat activity. For example, acoustic methods allowed the detection of sound produced by fish trawling – an important

function for preventing illegal fishing activity. Acoustic sensors can easily separate fishing vessels from smaller vessels and go-fast boats and even separate similar boats with low and heavy loads and boats towing underwater torpedo-style cargo containers.

The acoustic system employs modern methods of signal processing developed for target detection, tracking, and classification. Data integration between the acoustic data with other sensors is applied to generate an alert and target contact reports that can be sent to an appropriate operations center.

The suggested BDS system has the following advantages:

- The main detection sensors are radar and acoustics. Cameras have a limited field of view compared to the main sensors and are used for classification and identification of a Target of Interest (TOI). Cameras are directed to a TOI by the main sensors of the system. AIS is used to discriminate legitimate targets from potentially nefarious boats without AIS transmission, assuming AIS is not being spoofed and can be relied on to represent a legitimate target. With AIS, spoofing the BDS system can detect inconsistencies in the target positions and features (target visual and acoustic signatures) that lead to discrimination of potentially nefarious boats.

- The suggested BDS works in an autonomous regime. It does not require a human in the loop. The system sends an alert and contact report with target images to a command center.

- Acoustic sensors provide additional information about targets for their classification and allows for the separation of various classes of vessels based on their acoustic signatures.

- Acoustic methods can provide information about vessel activity such as fish trawling, go-fast boats, SPSS, LPV and other narco-submarines. Acoustic sensors can detect a vessel towing underwater torpedo-style cargo containers.

There is currently no low-cost system available on the market to provide autonomous and persistent maritime domain surveillance for the detection and classification of small boats, go-fast boats, and semi-submersibles. This research will contribute to testing the applicability and practicality of such a system for use by the USCG to detect illegal traffic.

This system can be installed on operational or abandoned oil rigs, various meteorological and navigation buoys, and remote shore locations. The sensors that comprise the system can be installed on land in remote areas, on oil rigs, on various stationary and non-stationary buoys, and Unmanned Surface Vehicles (USV) (see Figure 2).

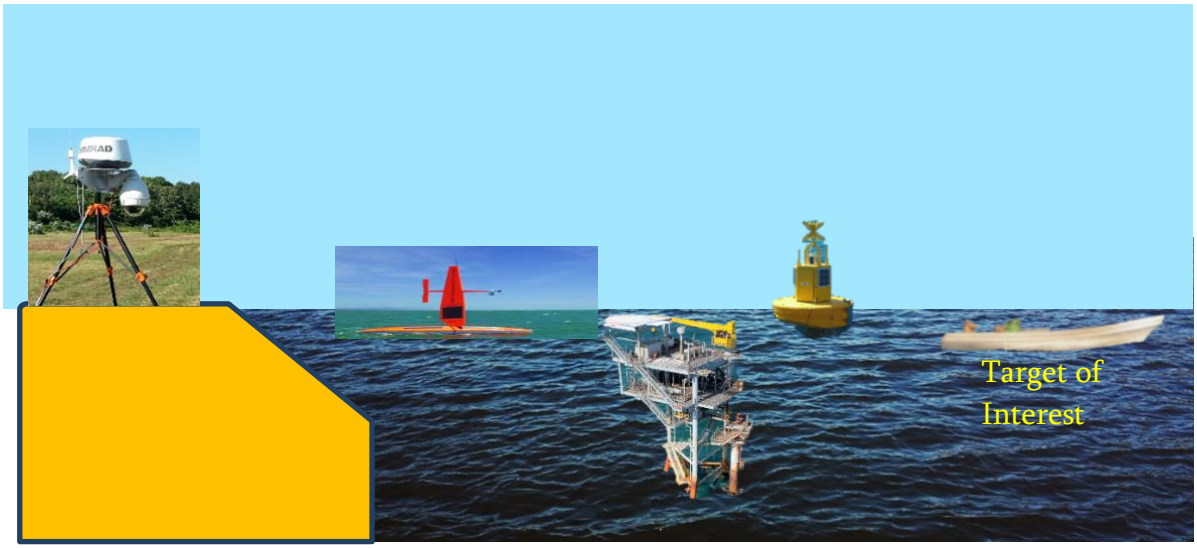



*Figure 2. Possible platforms for installation of low-cost Boat Detection System (BDS).*

### 2.1.4 Baseline

The USCG has various sensors installed on land, cutters, aircraft, helicopters, unmanned aircraft systems (UAS) and satellites that detect small illegal boats (Figure 3).


*Figure 3. USCG systems used for the detection of small illegal boats.*

These systems have several limitations:

- The land-based radar and EO/IR systems have limited coverage and can detect small boats in the proximity of a USCG sensor tower.

- These systems are ineffective for the detection of LPV, SPSS and narco-submarines.

- Aircraft and helicopter radar and EO/IR systems are expensive, and their operation is labor intensive and costly.

- UAS based sensors are less expensive, but still labor intensive since they require a team of UAS operators.

- Satellite images are expensive and satellite coverage is very limited and not always available.

A significant extension of sea surveillance with cost reduction can be achieved using a network of low-cost automated sensor systems. A majority of sensors in this system are independent COTS sensors that have been integrated and programmed with automated alert and detection capabilities. Since there were no COTS acoustic sensors that could be implemented in the suggested low-cost sensor suite, Stevens developed its Stevens Passive Acoustic Detection System (SPADES) practically from scratch.

A review of the state of art of available sensors for small boat detection and their parameters was provided in a previous MSC annual report submitted to DHS on August 31, 2020 and in the semiannual report submitted to DHS in December 2020.

The suggested low-cost automated sensor system has a cost that is several orders of magnitude lower than current land and air-based sensors and does not require a human in the loop for its operation. This system can be installed on abandoned oil rigs, various meteorological and navigation buoys, and remote shore locations (see Figure 2).

### 2.1.5 Methodology

This project's overall objective was to show a proof of concept of a low-cost sensor suite to assist the USCG and partner law enforcement agencies (e.g., CBP, ICE, police departments, etc.) to detect illegal maritime activity, such as drug trafficking, illegal fishing, and illegal immigration. The work methodology was based on the investigation of separate sensor performance (radar, cameras and acoustic sensors), development of software for multisensor data integration, alert and contact report generation, and detailed testing of the whole sensor suite in the real operational conditions in the Padre Island area and the Hudson River.

Several BDS with different sensors have been built and investigated. The simplest and lowest cost system (BDS1) consists of radar, camera, and AIS with software developed for automated boat detection. The Stevens cost of the system including sensors and computer is approximately $6,000, which is several orders of magnitude less than current sensors. Communication and power costs depend on the BDS carrier and are estimated at less

than $100 per month. This low cost allows the installation of a network of these systems to cover remote locations that are not covered by current expensive stationary optical and radar systems. We do not expect that the acquisition of multiple systems will further reduce the cost per unit.

The pictures of this low-cost systems installed at Stevens Babbio Center building and at Padre Island are shown in Figure 4.

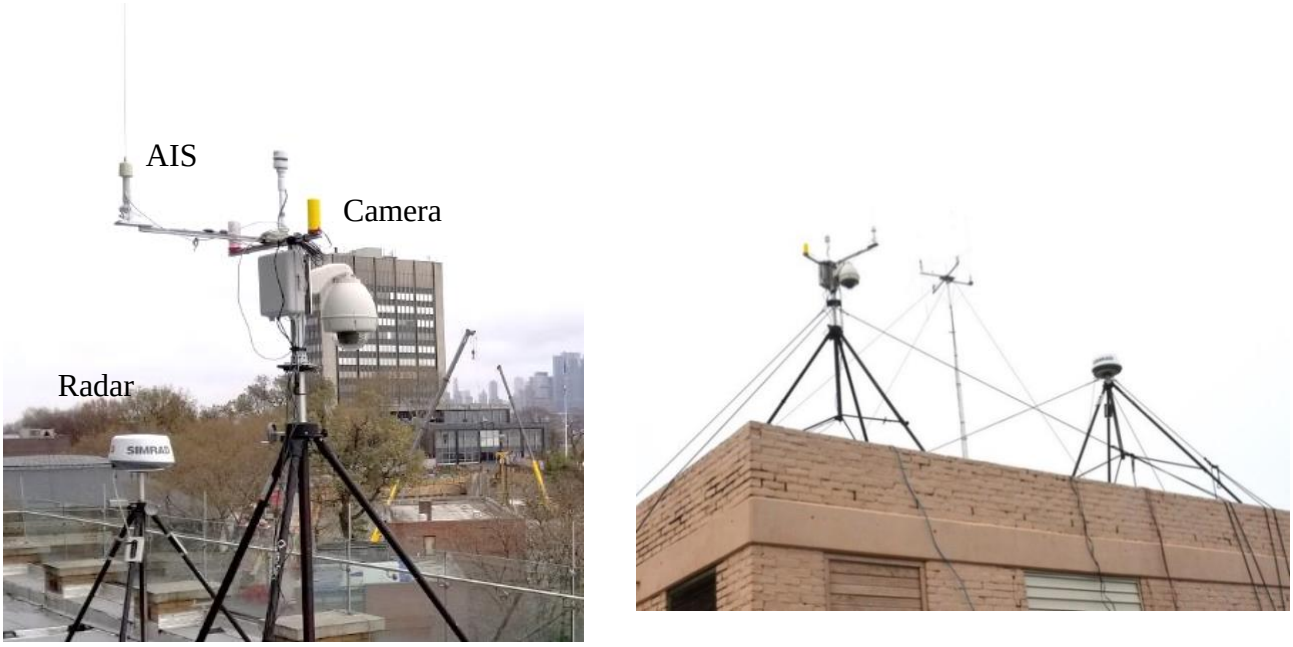



*Figure 4. A simplified version of BDS installed on the Babbio Center 6th floor patio (left) and on a shore-based location at Padre Island (right).*

Radar is the core sensor used by BDS1 for target detection and tracking. The low-cost radar does not provide digital signal processing required for automated TOI detection and tracking, so the Stevens research team developed an algorithm to provide this functionality and extend its integration with the other sensors. Three different radars were tested for the BDS systems: Simrad 4G, Simrad Halo 24, and Furuno DRS4D-NXT. Each of these radars cost approximately $2,000. The best performance was reached by the Simrad Halo 24 radar.

When a target is detected by the radar, the algorithm positions the optical camera in the direction of the Target of Interest and images of the tracked TOI are captured. While the algorithm generates target tracks from the radar, it also produces tracks using data collected from the AIS receiver. If a radar track is detected nearby an AIS track, the target is determined to have the respective AIS transmission. A detected target without AIS is an alerting sign for possible nefarious activity. The radar and AIS data are combined into a fusion tracker.

Contact reports are generated by the system after alerts or moments of interest featuring respective sensor data and captured images. The contact report is sent to a Command,

Control, and Communications (C3) center, and the results are viewable in the BDS graphical user interface (GUI). The algorithm, data processing, and report generation are performed by a dedicated processing computer that is part of the BDS. An example of the alert display is presented in Figure 5.

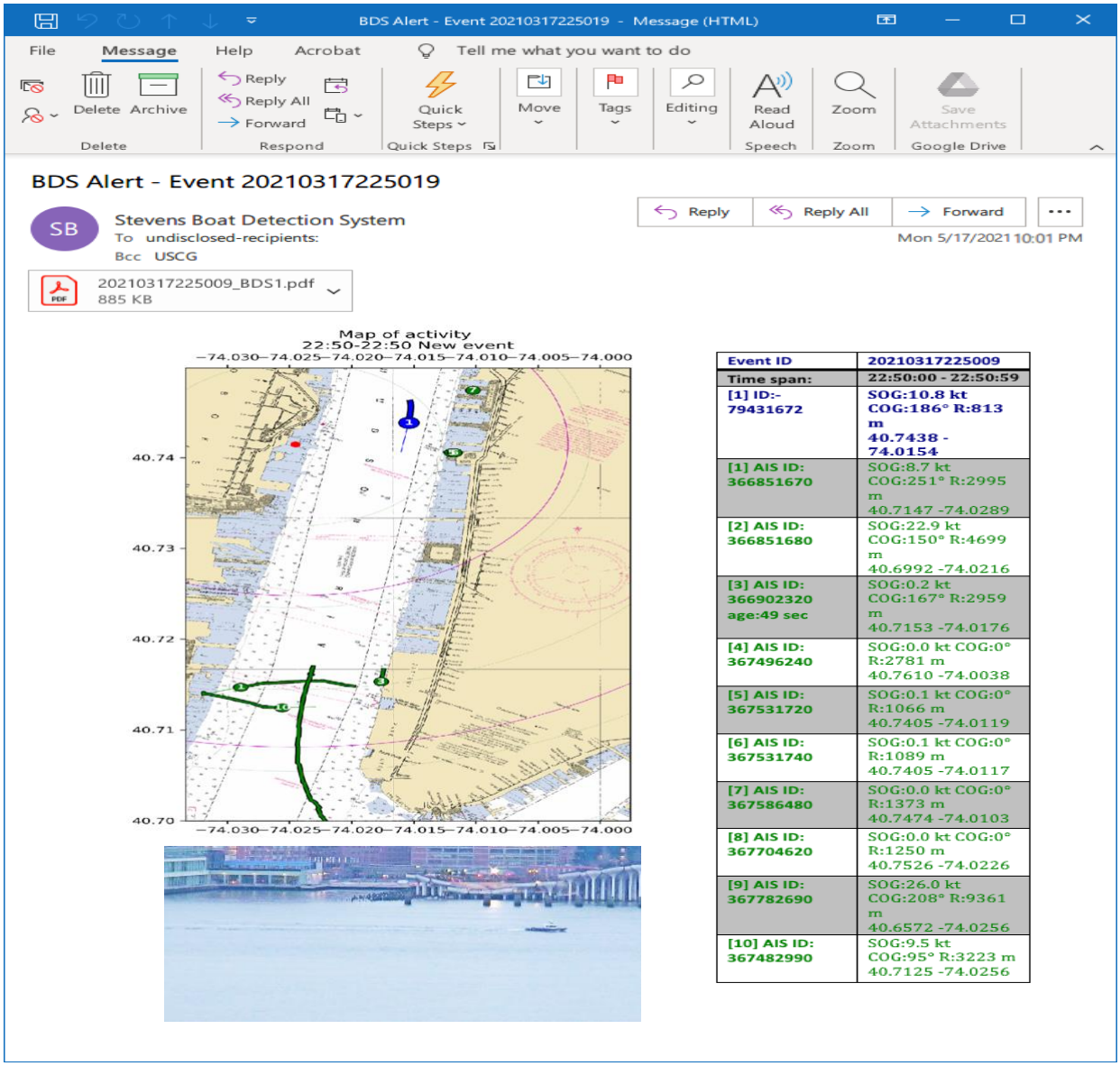



*Figure 5. BDS1 email alert for event 20210317225019 when a small boat coming into the radar LOS is detected (shown in blue). Vessels with AIS are marked in green.*

Several additional sensors were investigated for BDS applications. The additional sensors included three radars and an IR camera - FLIR RT-612E-NTSC PTZ IR that is a pan-tilt-zoom dual camera providing visible (VIS) and long-wave infrared (LWIR) thermal imaging (see Figure 6).

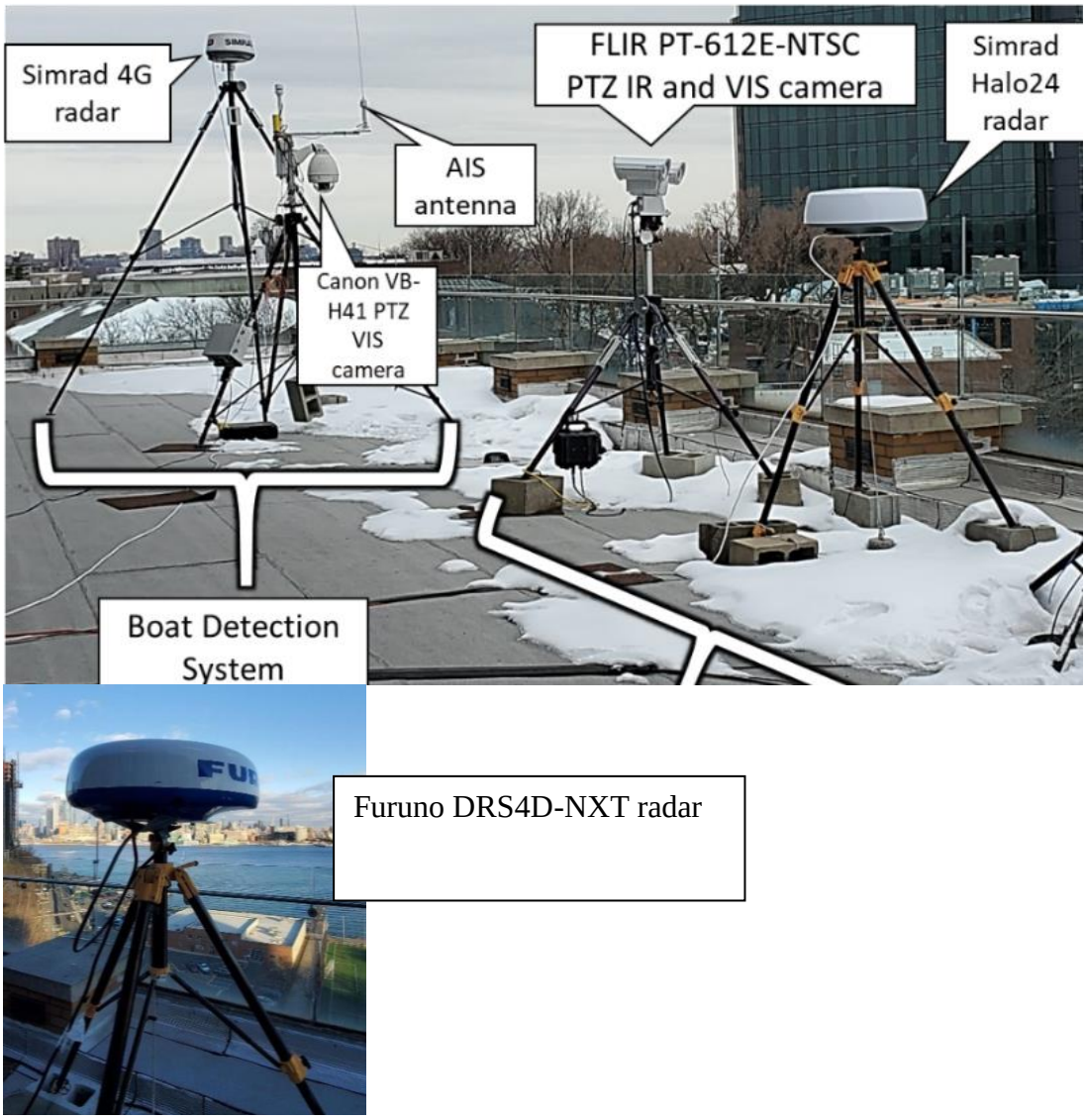



*Figure 6. BDS1 installed at Stevens with additional sensors and Furuno DRS4D-NXT radar.*

At Stevens, the BDS1 system was deployed on a 6th floor patio at a height of approximately 39 m Mean Sea Level (MSL). This deployment allowed a partially obscured view of the Hudson River as shown in Figure 7. The deployed system provided an opportunity to detect boats with Line of Sight (LOS) at a distance of 1.5 km to the North and 6 km to the South.

Even though the view was obstructed by buildings and their shadows, the prolonged deployment of the system allowed a diverse set of targets including vessels with and without AIS to be captured.

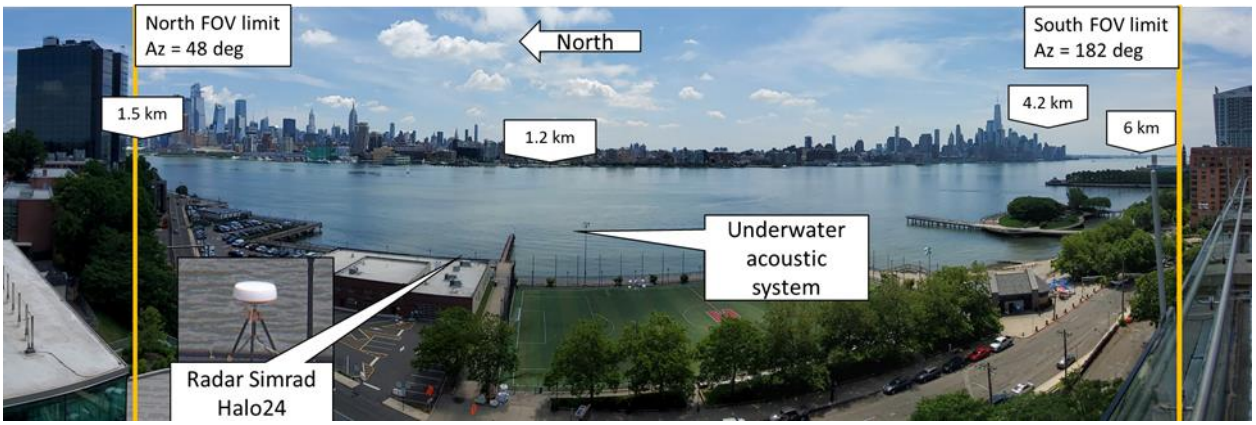



*Figure 7. Field of view from the BDS system installed on the Babbio Center patio facing East.*

The full BDS2 expands on BDS1 capabilities with the additional acoustic sensor, Stevens Passive Acoustic Detection System (SPADES-2).

The SPADES-2 array was improved from its previous iterations and tested in the Hudson River. The number of hydrophone channels were increased from four to eight which improved the detection reliability (see Figure 8).

The SPADES-2 that was deployed in the Hudson River uses a 150-meter cable which can be extended to 1000 meters if necessary. SPADES-2 is outfitted with Stevens homemade hydrophones featuring an extended reception frequency band.

SPADES provides azimuth, elevation, and amplitude information at the moment of detection. This data is visualized on the maps contained in the contact reports, alert emails, and GUI as beams in the direction of the detection at the time. The contact report also shows the acoustic detection data graphically over time alongside the fused track information from the radar and AIS.

The cost of the SPADES-2 components for a single node is about $11K, which makes the total cost of the BDS2 as $17K. The maintenance of SPADES is more complicated than the maintenance of BDS1 since water weeds and mussels can adhere to the underwater system and that can decrease its performance. Figure 9 shows SPADES extracted from the Hudson River after 7 months of exploitation. A lot of weeds are attached to the system, but they did affect the system performance. Periodical SPADES treatment, cleaning and re-deployment is required. We estimate that this can be done every 6 months using a small boat with 2 people and requiring 2-3 hours.

A network of sensors can use several sensors (nodes). We do not expect that the acquisition of multiple sensors further reduces the cost per unit.

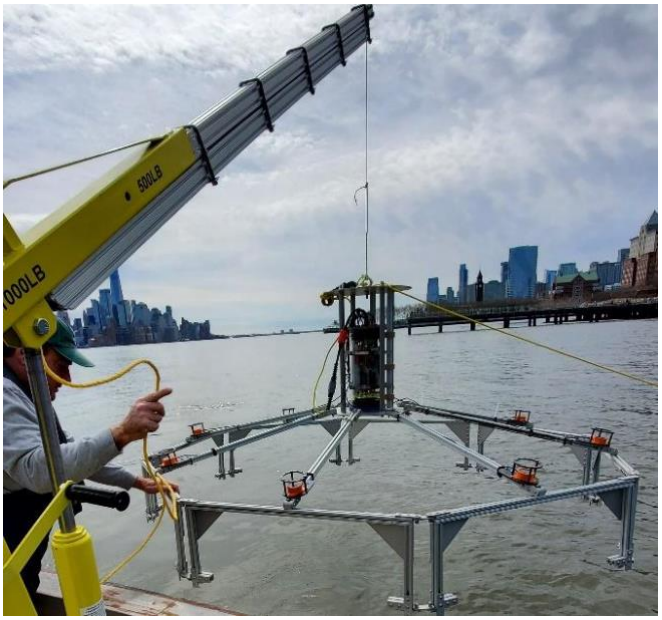



*Figure 8. SPADES-2 during deployment in the Hudson River.*

*Figure 9. SPADES-2 after 7 months of deployment in the Hudson River.*

The data from acoustic, optical and radar boat signatures collected in the Padre Island and in Hudson River tests were used for the development of special software for automated acoustic, optical and radar target detection, tracking and classification. Data integration of the acoustic data with other sensors was applied for the development of software generating a target contact report that can be sent in the form of an alert to an appropriate operations or command center.

### 2.1.6 Milestones and Performance Metrics

The project milestones that were identified in the work plan were modified in June 2020 taking into account COVID-19 related work restrictions. The milestones and the performance metrics were reviewed with the USCG and DHS representatives and were approved in the MSC Year 7 Work Plan. The milestones according to this plan are shown in Table 1.

*Table 1. Milestones according to the MSC Year 7 work plan.*

| No. | Milestone | Time Frame |
|---|---|---|
| M1 | Kick-off meeting to discuss project plan, objectives, and outcomes | Sept. 2019 |
| M2 | The experimental sensor suite showing data recording from radar, optical and acoustic sensor for detection tracking and classification of surface and underwater targets will be built and successfully deployed in the Padre Island National Seashore area. | Feb. 2020 |
| M3 | The advanced prototype algorithms and prototype software showing surface and underwater target detection, tracking and classification for radar, optical camera and acoustic sensors. The data fusion algorithm will generate an alert (contact report) that could be sent to law enforcement for illegal traffic interdiction. | Dec. 2020 |
| M4 | The sensor suite prototype will be capable of operating in an unattended mode enabling reliable, persistent detection of vessels | March 2021 |

All milestones of this plan were successfully completed. The simplified Boat Detection System (BDS1) was installed on the Stevens Babbio Center patio in June 2020 and the acoustic SPADES-2 was deployed in the Hudson River on March11, 2021. The full BDS is continuing to collect vessel radar, optical and acoustic signatures after the project was completed.

Stevens conducted additional research that was not included in the MSC Year 7 work plan. The additional research included:

1. Test of three different radars and choosing the most optimal among them. The best BDS performance was reached using a Simrad Halo 24 radar.

2. Investigation of IR camera applications for a low-cost sensor suite. The IR camera provides much lower resolution than the optical camera and the price of the IR camera is about 10 times higher, so IR is less suitable for a low-cost boat detection system. The acoustic system and radar provide 24/7 surveillance and a relatively expensive IR camera does not add much to the BDS performance.

3. Development and testing of the Stevens homemade low-cost hydrophones. The high-quality hydrophones used in the previous version of SPADES (ITC 6050C hydrophones) are rather expensive having a cost of more than $8K each. The cost of eight hydrophones for the new SPADES would have been more than $64k, which is too expensive for a low-cost system. Stevens has developed and built its own hydrophones that provided the same quality for a much lower cost. This allowed the research team to reduce the cost of one SPADES node to $11K.

According to MSC's Year 7 work plan, Table 2 lists the performance metrics used for measurement of the BDS effectiveness:

*Table 2. The performance metrics according to MSC's Year 7 work plan.*

| No. | Performance Metric | Time Frame |
|---|---|---|
| P1 | An alpha version of the integrated sensor suite will be installed at Stevens and will provide collection of acoustic, radar, optical and IR signatures of boats moving on the Hudson River for at least 3 months. System parameters measured will include detection, tracking and classification distances, probability of detection, and false alarm rates. These will be measured for different types of vessels under different weather and water conditions and at different times of day. Our goal is to detect small vessels up to 5 km away from the sensor with false alarm rates less than one alarm in 12 hours. The constant ship presence in the Hudson did not allow for the estimation of false alarm rates. | Nov. 2021 (Note that the system was deployed and operated for a much longer time than was initially planned in the workplan) |
| P2 | Acoustic, radar and optical signatures of various vessels will be collected for at least 50 boats of various types passing within range of the sensor suite. | March 2021 |
| P3 | Conduct the prototype system evaluation according to System Usability Scale. | March 2021 |

**Performance metrics observed in the tests:**

The results of the research conducted demonstrated the following performance metrics:

**P1.** The BDS1 with radar, camera and AIS was installed in the Stevens Babbio Center patio in June 2020 and provided data collection for radar, optical and IR signatures of

vessels moving on the Hudson River for a year. The acoustic system SPADES-2 was deployed on March 11, 2021 and is recording acoustic signatures. Information about the collected signatures is presented in the Low-Cost Covert Sensors for Remote Locations final report presented to DHS in June 2021.

The test conducted at real operational conditions in Padre Island demonstrated that acoustic sensors detected a small boat at a distance of about 8 km, which exceeds planned detection distances. The tests in the Hudson River did not allow finding the maximal detection distance because there were always several vessels present producing strong noise. NYC urban noise and traffic also produce strong noise.

**P2.** During the long-term deployment of the BDS in the Hudson River, acoustic, radar and optical signatures of various vessels were collected for more than 100 vessels as various types were passing within range of the sensor suite. The SPADES-2 is still collecting acoustic signatures and the system retrieval is planned soon.

**P3.** The planned system evaluation by USCG personnel did not take place due to COVID-19 travel restrictions. Additionally, USCG personnel could not visit Stevens for the system evaluation.

### 2.1.7 Transition Considerations

The developed low-cost system can be installed on oil rigs, various meteorological and navigation buoys, and remote shore locations. The sensors of the system can be installed on land in remote areas, on oil rigs, on various buoys, and Unmanned Surface Vehicles (USV).

There are many similar platforms near the USCG area of interest. Figure 9 shows a map of abandoned oil rigs and ATON buoys near the Mexican border in the USCG Sector Corpus Christi AOR.

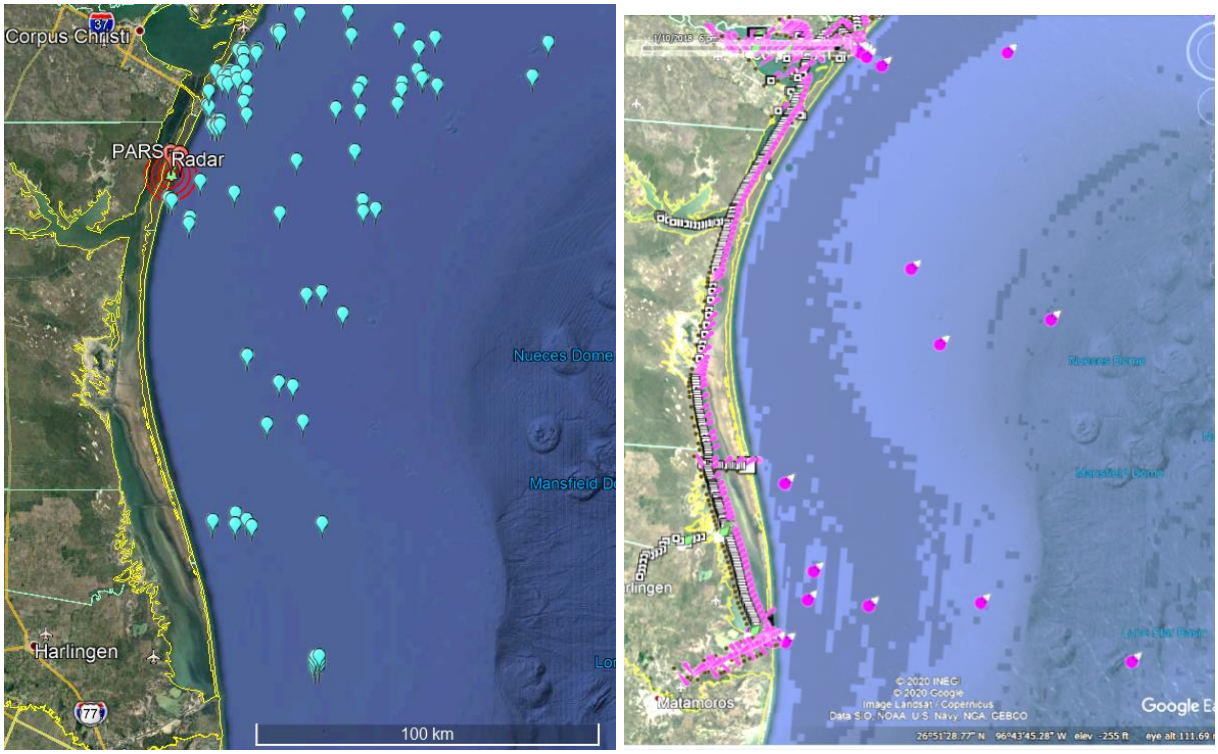



*Figure 9. Maps of abandoned oil rigs (left) and ATON buoys (right) near the Mexican border in the USCG Sector Corpus Christi AOR that can be used as a platform for the BDS sensor.*

The proposed experimental sensor suite uses low-cost COTS sensors including a marine radar, optical and infrared cameras, and AIS receivers in conjunction with a tethered underwater acoustic array, the Stevens Passive Acoustic System (SPADES) prototype, outfitted with low-cost hydrophones.

Several USV and UUV have been developed for ocean investigations and surveillance and many of them have acoustic sensors. These sensors are used for Anti-Submarine Warfare (ASW) and for marine mammals' investigation. The research team is not aware of applications of USV/UUV acoustic sensors for illegal boat detection. Figure 10 shows pictures of a USV with acoustic sensors. Two companies (Exocetus and SubSeaSail) asked Stevens researchers for assistance with acoustic boat detection software and organization of experiments demonstrating the performance of the acoustic sensors for illegal boat detection. Exocetus Autonomous just conducted a small boat detection test using acoustic sensors installed on the MOD2 glider (see Figure 10c). Exocetus followed the Stevens research team's recommendations in this test and provided Stevens with recorded data showing the feasibility of small boat detection by acoustic sensors. Future work could be conducted with these companies to demonstrate autonomous USV/UUV with radar, optical and acoustics automated detection and reporting of illegal boat activity.

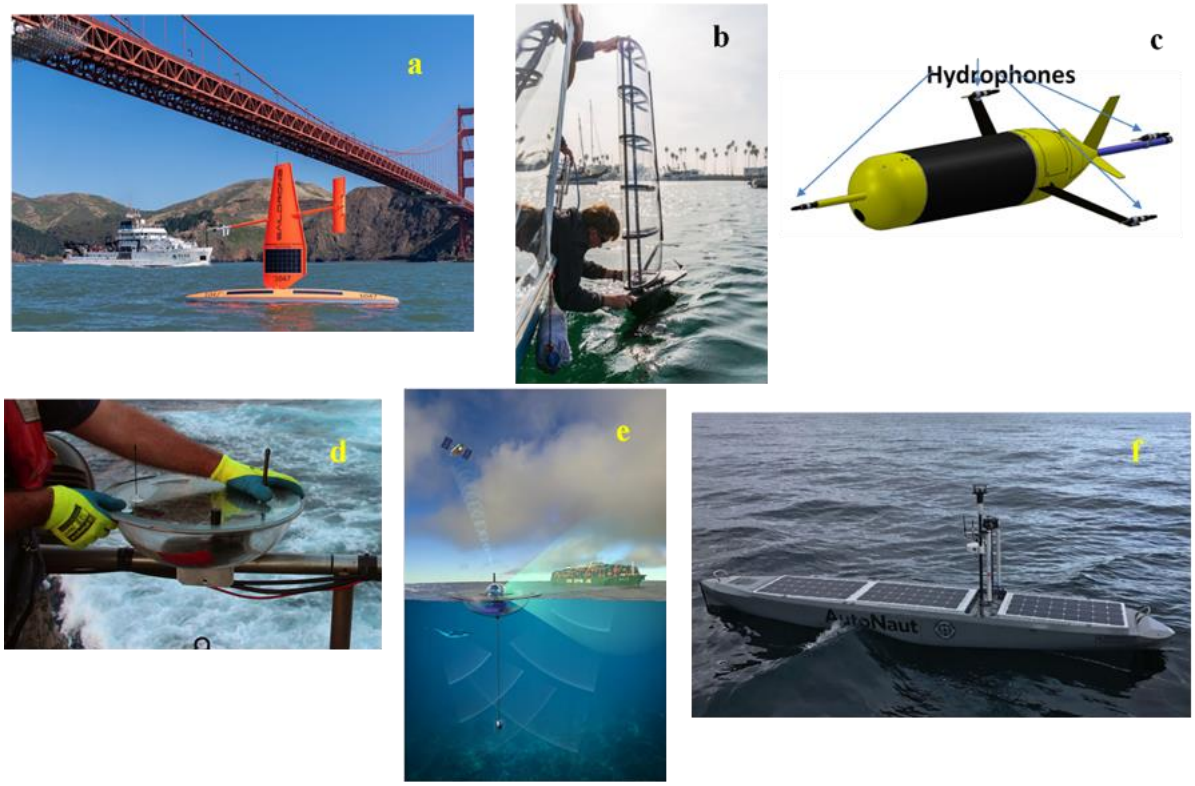



*Figure 10. USV with acoustic sensors:* ***a)*** *Saildrone USV can operate at sea as long as 12 months****. b)*** *SubSeaSail USV****. c****) Exocetus Passive Acoustic Monitoring Glider,* ***d,e)*** *The most unexpensive USV and sensor developed in DARPA project Ocean of things.* ***f)*** *AutoNaut Islay USV.*

The suggested low-cost sensor suite will effectively improve surveillance, detection, classification, and identification of vessels both on and below the water surface and to enhance homeland security mission capabilities in providing persistent surveillance of ports, coastal approaches, maritime sanctuaries, protection of sunken military vessels and wrecks, fisheries, and in the detection of smuggling activities, and will reduce personnel costs without degrading mission performance.

Given the state of maturity of the developed sensors and the experience the Stevens research team has in transitioning solutions to an operational setting, the team feels that this solution has a path to be successfully transitioned to the USCG. Also, given that the system does not need to use USCG operational data or its network, it makes transition easier and quicker.

**Intellectual Property Management Plans**

The principles of acoustic target detection are based on two Stevens patents:

1. Salloum, H., Sedunov, A., Sedunov, N. and Sutin, A., Stevens Institute of Technology, 2017. Passive acoustic detection, tracking and classification system and method. U.S. Patent 9,651,649.
2. M. Bruno, B. Bunin, L. Fillinger, H. Goheen, A. Sedunov, N. Sedunov, A. Sutin, M. Tsionskiy, J. Turner, M. Kahn, H. Salloum. Passive acoustic underwater intruder detection system. Patent number: 8195409. Issue date: Jun 5, 2012.

During the work on the project, numerous improvements to the existing SPADES have been made. Some of these improvements are included in the patent application by H. Salloum, A. Sedunov, N.Sedunov, A.Sutin "Directional acoustic signatures and source level measurements by passive acoustic system with few sensors" that was filed with the Stevens patent office. The suggested patent presents an extension of the two Stevens patents. The suggested disclosed subject matter relates to a high-resolution low-noise multidimensional system and method for measurement of acoustic signatures and intensities of acoustic, seismic, and/or hydro acoustic waves to detect the presence of man-made or natural sources of acoustic emissions that are used for classification of the type of source causing the emissions.

**Market Specific Considerations**

This project's main goal is to prove the concept of a practical, low-cost sensor suite for assisting the USCG in their drug interdiction mission. We expect that the applicability of the work, the practicality of the system, and the ease of operation will be discussed with the USCG to determine a transition path and requirements.

If the system provides the functions and performance needed by the USCG, the research team will seek a company to license and manufacture the sensor system. Our priority will be given to companies that have been selling maritime products to the USCG. Then the existing USCG acquisition process can be used to purchase this system.

During the preparation stage for system manufacturing, we plan to prepare all system documentation as well as training materials as we have done in the past for similar systems and provide these as part of the transition for future phases of this work. These will include the following: principles of operation, system architecture, system specifications, system configuration and revision history, Level 3 drawing package, Interface Control Documents (ICDs), component supplier noted on drawings, set-up/tear down manual, permission to operate, operator manual, maintenance and spares requirements for 3 years of operation. The software will be prepared as an executable package with installation and user manuals for the USCG to evaluate.

### 2.1.8 Stakeholder Engagement

The USCG is the primary stakeholder for this work. Implementation of autonomous low cost BDS will highly improve detection of illegal boat activity and threat of sea-based drug smuggling. Acoustic sensors in the low-cost sensor suite are especially important for detection of SPSS, LPV and small submarines that are considered by the intelligence community as possible tools for terrorist attack on the United States.

The USCG is the primary stakeholder for this work. A possible list of stakeholder organizations may include the USCG, NAVY, DoD Special Operations Command (SOCOM), Customs and Border Protection, Immigration and Customs Enforcement, Joint Interagency Task Forces, the Federal Emergency Management Agency, the U.S. Secret Service, the Domestic Nuclear Defense Office, the Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, Firearms & Explosives, the Department of Defense, DARPA, NOAA DOT Office of Maritime Security and the National Maritime Security Advisory Committee.

The need of the USCG for the suggested work has been articulated by USCG Sector Corpus Christi in discussions with researchers from Stevens. The Stevens team visited Corpus Christi in February of 2017, October of 2019 and in January of 2020. The USCG provided information needed about Targets of Interest (Lanchas), conducted helicopter surveillance of oil rigs, and provided access to the land deployment side. The team was able to gain first-hand insight into the terrain where illegal drug operations often occur in order to propose technical solutions to improve drug interdiction operations. The team also observed the environmental limitations, including access to the beach area, protected species, available locations for installation and communications, etc. associated with the geographical area.

The MSC team actively engaged the USCG stakeholders in this project. The USCG POC was engaged throughout the planning and execution of this project and has acted as the liaison with other USCG personnel.

### 2.1.9 Potential Programmatic Risks

The project has successfully completed. The final report and appendix included detailed technical system description have been submitted to DHS. The developed system including radar, camera and AIS installed on the Stevens Babbio Center patio and SPADES deployed in the Hudson River are continuing to collect vessel radar, optical and acoustic signatures beyond the completion of this project.

### 2.1.10 Progress Against Milestone Outcomes

All milestones were successfully completed on time.

### 2.1.11 Unanticipated Problems

The main unanticipated problems are the secondary effects due to COVID-19. Mainly, these were travel restrictions and the inability to use the Lab and machine shop. We addressed these problems according to our contingency plans and the MSC Year 7 work plan was successfully completed.

### 2.1.12 Information Supported by Data

The suggested low-cost sensor suite for illegal boat detection will effectively improve surveillance, detection, classification, and identification of vessels both on and below the water surface to emphasize illegal water traffic detection, illegal fishing and prevention of terrorist attacks from sea. This sensor suit will highly extend USCG capabilities for detection of SPSS, LPV and narco-submarines. Detection distances of these TOI by the developed acoustic sensor reach several tens of km.

The suggested sensor suite will also enhance USCG mission capabilities in providing persistent surveillance of ports, coastal approaches, maritime sanctuaries, protection of sunken vessels and wrecks, fisheries, and of smuggling activities and will reduce personnel costs without degrading mission performance.

Due to the low cost and simple installation of this system, it will allow permanent surveillance of a much larger ocean area than the currently used USCG sensors at a much lower cost. The developed automated algorithms generating alerts and contact reports allows extending surveillance without additional personnel.

The data collected during the Padre Island and Hudson River field tests demonstrates the feasibility of the suggested low-cost sensor suite for illegal boat detection and tracking. The long-term deployment in the Hudson River demonstrated the high reliability of the developed system.

**References**


- Bouma, H., De Lange, D., Broek, S., Kemp, R., Schwering, P., 2008. Automatic Detection of Small Surface Targets with Electro-Optical Sensors in a Harbor Environment. Proc. SPIE, vol. 7114
- Broek, S., Bouma, H. and Degache, M., 2008. Discriminating small extended targets at sea from clutter and other classes of boats in infrared and visual light imagery. Proc. of SPIE Vol. 6969.
- Brooke, J., 1996. SUS-A quick and dirty usability scale. Usability evaluation in industry, 189(194), pp.4-7.
- Cortese, F., Flynn, T., Francis, C., Salloum, H., Sedunov, A., Sedunov, N., Sutin, A. and Yakubovskiy, A., 2016, May. Experimental security surveillance system for an Island-based facility. In 2016 IEEE Symposium on Technologies for Homeland Security (HST) (pp. 1-4). IEEE.
- Dudzinski K M, Brown S J, Lammers M, Lucke K, Mann D A, Simard P, Wall C A, Rasmussen M H, Tougaard J and Eriksen N 2011 Trouble-shooting deployment and recovery options for various stationary passive acoustic monitoring devices in both shallow- and deep-water applications J. Acoust. Soc. Am. 129 436–48
- Ender, J., 2013. A Brief Review of Compressive Sensing Applied to Radar. Proc.14th International Radar Symposium IRS.
- Fillinger, L., de Theije, P., Zampolli, M., Sutin, A., Salloum, H., Sedunov, N. and Sedunov, A., 2010, November. Towards a passive acoustic underwater system for protecting harbours against intruders. In 2010 International WaterSide Security Conference (pp. 1-7). IEEE.

- Garnier, B., Andrisos, F., 2010.A Port waterside security systemic analysis. Proc. Waterside Security Conference (WSS).
- Gray, J., 2017. Canon continues developing their 250-megapixel APS-H sensor, offering exceptional surveillance capabilities. http://www.imaging-resource.com/news/2017/01/10/ canon-continues-developing-their-250-megapixel-aps-h-sensor
- Huang, W., Wang, D., Garcia, H., Godø, O.R. and Ratilal, P., 2017. Continental shelf-scale passive acoustic detection and characterization of diesel-electric ships using a coherent hydrophone array. Remote Sensing, 9(8), p.772.
- Moller-Hundborg, C., Thompson, A., Marqversen, O., Hansen, K., Pedrsen, M., Lokke, M., 2011. Small Target Detection with Scanter 5000 & 6000 Radar Series. Proc. 11th International Radar Symposium IRS.
- Rice, J., Wilson, G., Barlett, M., Smith, J., Chen, T., Fletcher, C., Creber, B., Rasheed, Z., Taylor, G., Haering, N., 2010. Maritime Surveillance in the Intracoastal Waterway using Networked Underwater Acoustic Sensors integrated with a Regional Command Center. Proc. Waterside, Security International Conference (WSS).
- Sousa-Lima, R.S., Norris, T.F., Oswald, J.N. and Fernandes, D.P., 2013. A review and inventory of fixed autonomous recorders for passive acoustic monitoring of marine mammals. Aquatic Mammals, 39(1), p.23.
- Stanistreet, J.E., Risch, D. and Van Parijs, S.M., 2013. Passive acoustic tracking of singing humpback whales (Megaptera novaeangliae) on a Northwest Atlantic feeding ground. PLoS One, 8(4), p.e61263
- Sutin, A., Salloum, H., DeLorme, M., Sedunov, N., Sedunov, A., Tsionskiy M., 2013. Stevens Passive Acoustic System for Surface and Underwater Threat Detection. Proc. Conf. of Technologies for Homeland Security (HST).
- Toet, A. and Wu, T., 2008. Small maritime target detection through false color fusion. Proc. SPIE, Vol. 6945-27, Optics and Photonics in Global Homeland Security IV, Orlando FL, USA.
- Sutin, H. Salloum, M. DeLorme,N. Sedunov, A. Sedunov, and M. Tsionskiy. Stevens Passive Acoustic Detection System for Surface and Underwater Threat Detection. 2013 IEEE International Conference on Technologies for Homeland Security (HST).
- A.Wignall, An Overview of ASW Sonobuoy Types and Trends, Technical Director at Ultra Electronics Ltd, Sonar & Communication Systems (2003)

## 2.2 RF Surveillance Project

PI: Tim Flynn, Stevens Institute of Technology
Project Period: September 2019 - December 2020
Budget: $264,852

### 2.2.1 Abstract

The USCG plays a crucial role in the nation’s efforts to interdict and counter dangerous narcotic drugs transported in maritime environments. Detection and monitoring of vessels trafficking narcotics occurs principally through the collection, analysis, and dissemination of tactical information and strategic intelligence combined with effective sensors operating from land, air and surface assets. The USCG is looking for low-cost, unmanned, maritime

domain awareness technologies and sensors that can provide an additional layer of intelligence and locate illegal boats and their shore accomplices.

Our work was focused on the development and building of a low-cost RF Surveillance System that can detect and find the direction to the source of RF signals. RF communication signals radiated from crews of illicit boats and by their accomplices can provide significant intelligence about the boat, its position, and its intent and may even be used to detect and localize persons waiting for illegal deliveries. Another application of detecting RF signals from smugglers relates to tactics that allow traffickers to leave a shipment at high-sea attached to GPS-enabled radio or satellite buoys. For this purpose, satellite and radio buoys adapted from the fishing industry are used and the RF surveillance systems developed can detect and localize RF radiation from these buoys.

The objective of this project was to investigate opportunities of radio monitoring and localization of various RF emitters onboard an illegal vessel, on shore and on RF buoys. This report presents the results of the MSC research aimed at the development of a low-cost Radio Frequency Surveillance System (RFSS). The primary objective of this project was to provide a proof of concept of an RF communication detection and RF direction finding system which is capable of detecting and localizing communications made by bad actors performing an illegal activity in the maritime environment. Another application of detecting RF signals from smugglers relates to tactics that allow traffickers to leave a shipment at high-sea attached to GPS-enabled radio or satellite buoys. For this purpose, satellite and radio buoys adapted from the fishing industry are used and the RF surveillance systems developed can detect and localize RF radiation from these buoys.

### 2.2.2 Changes from Initial Workplan

The unforeseen COVID19 pandemic has restricted the MSC's ability for development and building the RF Surveillance Systems (RFSS) due to limitations associated with laboratory and field tests. With the unavailability of the team to work in the laboratory, efforts were partially compensated by building small electronic laboratories at the homes of Stevens engineers. These small home laboratories allowed continuation of the RFSS development and testing but made this process slightly slower than originally planned. We were lucky that we managed to conduct the system sea test in Padre Island before the pandemic, even though this test was not included in the initial work plan. This test demonstrated the ability of our first version of the RF signal detector to detect RF communication signals from a small boat at distances up to 13 km.

During the pandemic, we paid more attention to the theoretical part of the work. We even extended this part from what was previously planned. The novel model for estimation of RF signal detection distances was developed and applied for real sea conditions in the proximity of the Padre Island National Seashore area. We developed an antenna simulator that provides simulation of the real RF signals for the system testing in laboratory conditions.

Although building the RFSS was delayed and the planned tests in NJ were postponed due to COVID-19 restrictions, Stevens built the RFSS system and completed its tests in the

Hudson River in the beginning of 2021. A brief system description and test results are included to this report.

### 2.2.3 Objective

The USCG plays a crucial role in the nation's efforts to interdict and counter dangerous narcotic drugs transported in maritime environments. Detection and monitoring of vessels trafficking narcotics occurs principally through the collection, analysis, and dissemination of tactical information and strategic intelligence combined with effective sensors operating from land, air and surface assets. The USCG is looking for low-cost, unmanned, maritime domain awareness technologies and sensors that can provide an additional layer of intelligence and locate illegal boats and their shore accomplices.

Our work was focused on the development and building of a low-cost RF Surveillance System that can detect and find the direction to the source of RF signals. RF communication signals radiated from crews of illicit boats and by their accomplices can provide significant intelligence about the boat, its position, and its intent and may even be used to detect and localize persons waiting for illegal deliveries. Another application of detecting RF signals from smugglers relates to tactics that allow traffickers to leave a shipment at high-sea attached to GPS-enabled radio or satellite buoys. For this purpose, satellite and radio buoys adapted from the fishing industry are used and the RF surveillance systems developed can detect and localize RF radiation from these buoys.

The objective of this project is to investigate opportunities of radio monitoring and localization of various RF emitters onboard an illegal vessel, on shore and on RF buoys. In this project, we are investigating various opportunities for the development of a radio monitoring system that can detect and localize different RF emitters on boats and emitters on shore (cellular and satellite phones, maritime communication systems, two-way radios, CB radio, GPS trackers using satellite or radio communications, etc.). The experimental RFSS setups were developed based on low-cost COTS components that enable building and field testing of a low-cost RF surveillance prototype. This project's goal is to prove the feasibility of a low-cost capability for RF signal surveillance. Modern electronics, computers and signal processing methods allow building such a system with features that are cheaper and comparable in performance with current Electronic Intelligence and Direction-Finding systems that are costly to acquire and operate.

An option of using small Unmanned Aerial Systems for recording RF signals was also investigated. A Software Defined Radio installed on the UAS was tested for recording and localizing RF communications signals from boats. This system can be used on a small tethered UAS and can highly extend the system's detection range and operation capacity.

This project provides a proof of concept for a low-cost method that will assist the USCG in detecting suspicious boats at distances exceeding detection ranges of current systems, will allow detection of GPS buoys, and will provide additional intelligence that can assist in increasing the narcotic and human traffic interception rates.

Crews of boats involved in illegal activities may communicate with their accomplices on other boats or on land. The ability to intercept RF signals used in communications and locate their source can be used for illegal boat detection and interception.

Another application of RF signals by drug smuggler relates to new tactics that allow traffickers to leave illicit shipments (e.g., drugs) at high-sea attached to a GPS-enabled radio or satellite buoys. Satellite and radio buoys adapted from the fishing industry are used for this purpose. The application of the electronic system for Electronic Intelligence and Direction Finding allows the detection and localization of these buoys.

A review of RF communication systems that can be used by drug smugglers and in illegal fishing activity is presented below.

### *Citizen Band radio*

Drug smugglers may consider CB radio as the most suitable communication system. This system works in the range of 27 MHz which is not typically monitored by the USCG. The number of RF stations in this frequency range is much lower than that in the frequency range of two-way VHF and UHF radio. CB radio is one the most widely used communication systems, frequently utilized by long-haul truckers, hunters, and off-roading enthusiasts[2]. This system operates on AM modulation with 4 watts of transmit power in the frequency range from 26.965 MHz (Ch 1) to 27.405 MHz (Ch 40). It does not require a license in the US and can be used for commercial and personal communications.

Any channel may be used with either single or double-sideband amplitude modulation except Channel 9, which is reserved for emergency communications. CB stations are limited to 4-watt carrier waves output power on Double Side Band (DSB) AM and 12-watts Peak Envelope Power (PEP) on Single Side Band (SSB) AM. The usable reliable range of CB on the water is about five miles but a higher antenna on land can provide a longer communication distance (see project final report). An abandoned Panga with a $2 million-plus load of marijuana was found in California's Monterey County on the Big Sur coastline. A CB radio was found on a beach near the Panga boat. The smugglers were arrested in a van. Inside the van, deputies found a CB radio tuned to the same channel as the CB radio found on the beach.

There are several pitfalls to having a CB radio on the water. Channel noise and station traffic are sometimes heavy, and the Coast Guard does not monitor the emergency channel. A similar frequency is used in radio buoys. For example, Longline HF Radio Buoy WamBlee uses a frequency between 26.8 and 27.2 MHz, with RF power of 4W. It uses AFSK modulation and has a programmable transmission rate of a minimum of 10 minutes and a maximum of 6 hours. Information is transmitted in an encrypted format and can only be decrypted by the radio beacon owner. Transmission times are also suitably optimized to prevent interception. The radio buoy with the W880 radio beacon can operate for up to 10 days with a coverage of 80 Km, as reported by the manufacturer.

### *Two-way VHF and UHF radio*

The low-cost and widely used two-way VHF and UHF radios are popular in marine communication. The two most commonly used frequency ranges for two-way radios are VHF (Very High-Frequency at 130-174MHz)**,** and UHF (Ultra High-Frequency at 400-520MHz)[5]. For example, a 25-watt marine radio will roughly have a maximum range of 60 nautical miles (111 km) between antennas mounted on tall ships, but that same radio will only have a range of 5 nautical miles (9 km) between antennas mounted on small boats at sea level.

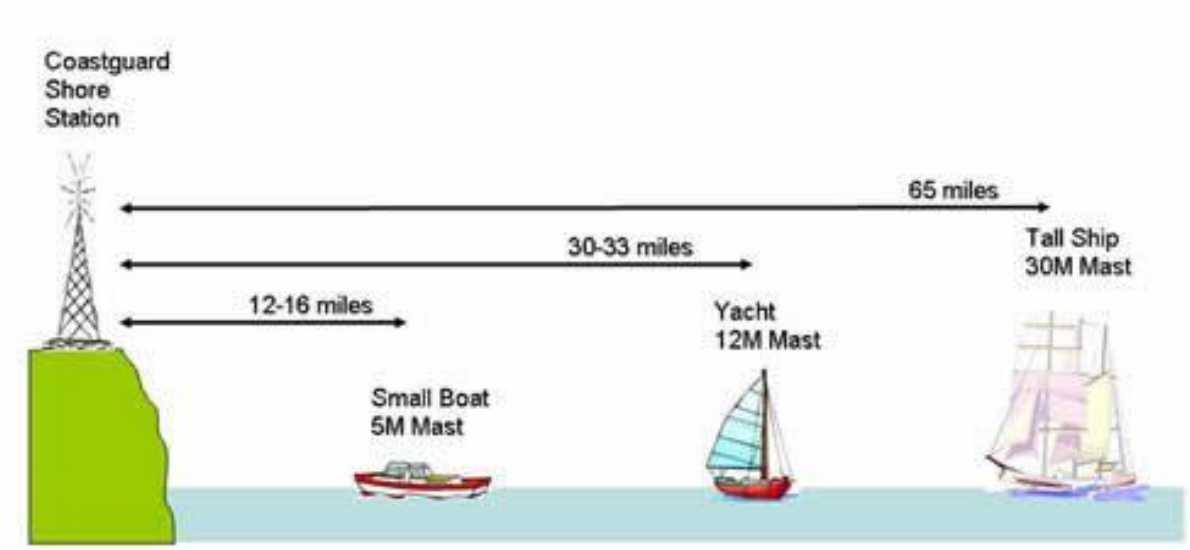



*Figure 1. Communication distances for two-way VHF and UHF radios [5].*

Table 4 presents an overview of service RF bands in the US that can be used by crew boats involved in illegal activity.

*Table 4. Overview of service RF bands in the USA*

| Service | Band & Frequency Range ** | License Required | Max Channels | Max Watts | Usage Type | Comments |
|---|---|---|---|---|---|---|
| FRS | UHF 462 & 467 MHz | No | 22 | 2 | Personal or business | New changes to this service allow it for business. [3] Channels 8-14 must be ½ watt. |
| GMRS | UHF 462 & 467 MHz | Yes | 22 +8 repeater | 50 | Personal only | Licensee must be 18 years or older. Anyone, regardless of age, can operate your radios. |

| | | | | | | |
|---|---|---|---|---|---|---|
| LMR | VHF 150-174 MHz UHF 421-512 MHz | Yes | 512 | 100 + | Business or government | Licensee must be 18 years or older. Also called PLMR. |
| MURS | VHF 151 & 154 MHz | No | 5 | 2 | Mixed use | Limited range. * External antenna up to 60ft to extend range. |
| Marine | VHF 156 - 162 MHz | No | 48 | 100 + | Mixed use | Only use marine radios. [3] All marine radios have the same pre-set channels & frequencies. |
| CB | HF 26.965 - 27.405 MHz | No | 40 | | Mixed use | All CB radios have the same pre-set channels & frequencies. |

Two-way radios are widely used in criminal activity. For example, the Mexican criminal cartel Los Zetas built a radio network in Matamoros, a border city across from Brownsville, Texas, around 2004. Initially, the small cluster of radios and antennas were tools to monitor police and other drug gangs. Mexican soldiers raided a Los Zetas-occupied home that contained networked laptops, 63 digital walkie-talkies, a central processing unit to remotely control repeaters, and a digital radio that communicated with airplanes. A recent paper describes how the Mexican cartel had installed its own antennas on a cellular tower in rural Mexico to support their two-way radios. In addition to high-end encrypted cell phones and popular messaging apps, traffickers still rely heavily on two-way radios like the ones police and firefighters use to coordinate their teams on the ground. One engineer who spoke with Reuters estimated that Cartel parasite antennas are present on roughly 20% of towers where his firm works, while another said about 30% of his sites had them when local criminals were particularly active in his area in 2018. VHF radio is also used in radio buoys that can be used by drug smugglers for tracking cocaine shipments at high seas.

The Chinese e-commerce company Alibaba is selling the GPS RD210 Fishing Net Tracking Buoy Integrated GPS & VHF Antenna to Transmit Full AIS Messages to Track Small Vessel Software for $183.26. This buoy has up to 12nm range with working frequencies of 161.975MHz / 162.025MHz and position update every 3 minutes.

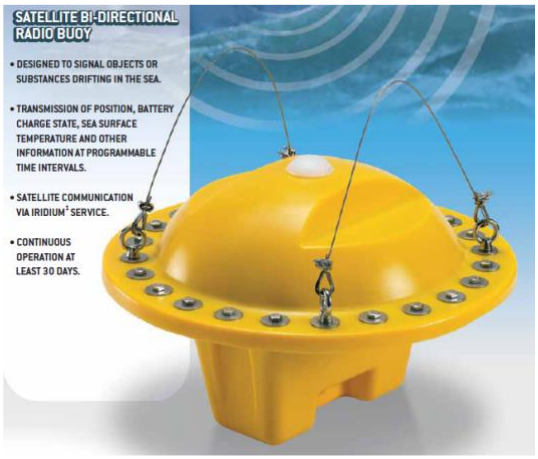



*Figure 2. W810 radio buoy produced by WanBlee*

### *Satellite phone*

Satellite phones provide reliable communication from any point on Earth and were found on a smuggling boat intercepted by the USCG. The frequencies of various kinds of satellite phones are presented in the table below.

*Table 5. Frequencies of various kinds of satellite communication*

| Satellite Communication type | Frequencies, MHz |
|---|---|
| Iridium | 1616 - 1626.5 |
| Inmarsat and LightSquared | 1525 -1646.5 |
| Thuraya | 1525 – 1661 |

Satellite communication is also used in various RF buoys that can be used by drug smugglers. One of these buoys, W810, produced by WanBlee, is a radio beacon that works through Iridium satellite coverage to ensure signaling and remote localization of objects or substances abandoned at sea. By sending out a message at programmable time intervals, it is possible to determine, via an electronic messaging system, an object's location, time of detection, battery charge state, and water surface temperature (provided that the special option has been installed).

Additionally, a flashlight indicator, which can be activated continuously or via a message sent through Iridium, enables drifting objects to be easily located also at night-time or under poor visibility conditions. Any information received from the W810 radio beacon is available through the Iridium system or its own messaging system which, upon a customer's request, can also forward the received information by email, SMS, or Inmarsat.

Next, a short review of signal intelligence, direction finding, and RF source localization is presented.

Application of electronic equipment for intersecting RF communications and locating sources of RF signals has a long history. The history of Electronic Intelligence, Electronic Warfare and Direction Finding is presented in many papers and books (see for example [10]). The first electronic interception took place around 1900 during the Boer Wars. The British Royal Navy had installed wireless sets produced by Marconi on board their ships in the late 1890s where limited wireless signaling was used by the British Army. Some wireless sets were captured by the Boers. The birth of signal intelligence in a modern sense dates to the Russo-Japanese War of 1904-1905. As the Russian fleet prepared for conflict with Japan in 1904, the British ship HMS Diana stationed in the Suez Canal, for the first time in history, intercepted Russian naval wireless signals being sent out for the mobilization of the fleet. In 1915, several stations were built in the UK for interception of German U-boat communications and for determining their location.

The USCG is first in the U.S. to intercept ships during the 1920s and 1930s by relying on signals, successfully reducing a massive flow of illegal smuggling along the 12,000-mile coastline by 60 percent.

Interception and intelligence analysis of communications from illegal boats is a significant part of the USCG intelligence [11]. The USCG gathers Signals Intelligence information from data transmissions, including communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT) using sophisticated equipment installed on USCG cutters and aircraft.

The USCG resources for Signal Intelligence can be used for the detection and tracking of communication from illegal boats and detection of radio buoys, but they are expensive and require highly trained personnel. Cheaper methods of RF signal detection and direction-finding can be developed that provide automated detection of boat and buoy signals. Many systems can detect and find direction to an RF source of radiation. These systems are used for various purposes, but one important application of these systems is the detection of radio frequency (RF) jammers and other sources of interference. Recently, the National Urban Security Technology Laboratory (NUSTL), a U.S. Department of Homeland Security lab, published a market survey report of RF detection, spectrum analysis, and direction-finding equipment that can be used to detect, identify, and locate RF interference sources that may be disrupting first responder communications systems. The purpose of this market survey report is to provide emergency responders with information on RF detection, spectrum analysis, and direction-finding equipment that are commercially available in order to guide purchasing and acquisition decision-making [12]. Table 6 shows a comparison of these COTS systems and their prices.

*Table 6. COTS RF monitoring and direction finding system*

| Manufacturer | Product | Price | RF Detection | Spectrum Analysis | Direction finding | Built-in display | Detection Bandwidth* | Scanning Bandwidth* | Receiver Sensitivity |
|---|---|---|---|---|---|---|---|---|---|
| Alion | Versatile RF Automated Monitoring System | $76,270.53 | ✓ | ✓ | ✓ | | 20 MHz to 6 GHz | 10 Hz to 650 kHz | 22 dB, centered at 2 GHz |
| Applied Signals Intelligence | ASI 2020DF Fixed Site | $125,000 | ✓ | ✓ | ✓ | blank | 2 MHz to 600 MHz | 1 MHz | -134 dB to -123 dB |
| Applied Signals Intelligence | ASI 2020DF Backpack | $100,000 | ✓ | ✓ | ✓ | | 2 MHz to 600 MHz | 1 MHz | -134 dB to -123 dB |
| Chemring Technology Solutions | Resolve 3 HF/VHF/UHF Direction Finding System | $150,000 | ✓ | ✓ | ✓ | blank | MHz to 3 GHz (detection); MHz to 3 GHz (direction finding) | 40 MHz | <20 dB to <6 dB, dependent on frequency |
| CRFS | RF Eye Guard | $130,000 | ✓ | ✓ | blank | blank | Dependent on RF Eye Node integrated into the system | Dependent on RF Eye Node integrated into the system | Dependent on RF Eye Node integrated into the system |
| DGS | SigBASE 6000 | $50,629 | ✓ | ✓ | ✓ | blank | 50 MHz to 6 GHz | 20 MHz to 80 MHz | Dependent on transmission frequencies and antenna configuration |
| DGS | SigBASE 4000 | $15,999; $7,999 for software | ✓ | ✓ | | ✓ | 70 MHz to 6 GHz | 20 to 40 MHz | -114 dBm with 1 kHz bandwidth, centered at 2.4 GHz |
| LS Telcom | LS Observer | $27,600 (FMU); $34,500 (PPU); | ✓ | ✓ | ✓ | blank | 9 kHz to 18 GHz (FMU | 9 kHz to 6 GHz | Dependent on frequency |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | $33,400 (PMU) | | | | | and PPU); 9 kHz to 12.4 GHz (PMU) | (WB1 scanning mode); 100 kHz to 18 GHz (WB2 scanning mode); 100 kHz to 12.4 GHz (NB scanning mode) | |
| PCTEL | SeeWave Interference Locating System | $25,445 | ✓ | ✓ | ✓ | ✓ | 690 MHz to 6 GHz | 5 kHz to 20 MHz | -120 dBm to -30 dBm, centered at 30 kHz |
| Rohde and Schwarz | PR100 Portable Receiver | $24,000 | ✓ | ✓ | ✓ | ✓ | 9 kHz to 7.5 GHz | Contact Rohde and Schwarz for specifications** | Contact Rohde and Schwarz for specifications** |
| Rohde and Schwarz | DDF007 Portable Direction Finder | $150,000 | ✓ | ✓ | ✓ | ✓ | 9 kHz to 7.5 GHz (detection); 20 MHz-6 GHz (direction finding) | Contact sales rep | Contact sales rep |
| Rohde and Schwarz | NESTOR Mobile Network Survey Software and RF Scanner** | Contact Rohde and Schwarz for pricing* | blank | ✓ | blank | blank | 350 MHz to 4.4 GHz | 140 Hz to 1.438 MHz | -126 dBm with a 22.46 kHz bandwidth, centered at 900 MHz |

*This information was not given because it is considered proprietary or competition specific by the vendor.
**Specifications given for the R&S NESTOR reflect the typical configuration with the R&S TSMA Scanner.

| | |
|---|---|
| Acronyms:<br>FMU: Fixed Monitoring Unit<br>PPU: Protected Portable Unit<br>PMU: Portable Monitoring Unit<br>WB1: Wideband 1<br>WB2: Wideband 2<br>NB: Narrowband | Units: Hz: Hertz kHz: Kilohertz MHz: Megahertz GHz: Gigahertz dB: Decibel dBm: Decibel relative to 1 milliwatt |

These systems provide the detection of RF jamming and interference signals. These signals usually continue a relatively long time and can be detected using frequency scanning in a wide frequency band. This method does not work for short communication signals that can be radiated by smugglers and radio buoys.

The reception of short communication signals can be conducted in a narrow frequency band. The USCG uses RF detection and direction-finding systems for RF in several narrow frequency bands for detection and localization of emergency calls. The USCG has developed and built the Rescue 21 system providing detection and localization of emergency calls (Hebert 2016) . The USCG has conducted approximately 100,000 search-and-rescue (SAR) operations since 2006 with support from the Rescue 21 system. Rescue 21 helps identify the location of callers in distress via towers that generate lines of bearing to the source of VHF radio transmissions and significantly reducing search time. The goal of the system, according to the prime contractor General Dynamics, is to be able to "receive, at minimum, a one-second transmission from a one-Watt power source with an antenna two meters above sea level up to 20 nautical miles from shore". This system detects emergency signals only and is expensive with its current cost estimated at over $1B.

The DF-430 Multi-Mission Direction Finder is another USCG piece of equipment with direction finding capabilities. The DF-430 is specifically designed to receive and interrogate all current international distress frequencies including 121.5 MHz, 243 MHz, 406 MHz, as well as the ARGOS and COSPAS-SARSAT encoded beacon signals.

There are several integrated Maritime Security systems that use a Radio Direction Finder as one of the system sensor elements. One of these systems is the STYRIS®.  One Solution for Maritime Safety and Security. AIRBUS has a product line for collecting, processing, consolidating, enriching, distributing, and displaying data from a wide range of maritime sensors [(STYRIS®  2020). The software consolidates data gathered from sensors like radars, Automatic Identification System (AIS), Radio Direction Finders (RDF), cameras, weather stations, and sonars. Radio Direction Finders are sensors that support surveillance operations by finding the azimuth direction of a radio transmission source. The STYRIS® CSS RDF module is used to support routine surveillance missions, search-and-rescue, radio spectrum scanning, and interception of illicit communications. This system is also expensive and requires well-trained personnel.

The WD-3300, produced by MORCOM International, is a direction-finding system available on the market that could be used to detect communications from illegal boats and radio buoys (Fig. 3).

*Figure 3. The WD-3300 DF system 3300 produced by MORCOM international Inc.*

The WD-3300 system satisfies the need for a flexible, transportable, affordable, and easily deployable direction-finding system. It is a ruggedized, transportable DF system comprised of fully integrated receivers, battery, charging unit, and control circuitry in a compact sturdy carrying case, ready for quick and easy deployment anywhere, with or without external power sources. The system also has a high contrast display and standard laptop computer facilities which can integrate simultaneously with other applications. The unit contains one or more WiNRADiO card receivers which offer a wide frequency range from 20 MHz to 1.8 GHz. The receiver range is extendable to 3.5 GHz. The cost of WD-3300 with antennas covering 2-1000MHz is approximately $60k. This system has a high cost also and its application to USCG needs will require development and implementation of software for automated detection of short-duration signals and direction finding.

### 2.2.4 Baseline

Crews of boats involved in illegal activities may communicate with their accomplices on other boats or on land. The ability to intercept RF signals used in communications and locate their source can be used for illegal boat detection and interception.

Another application of RF signals by drug smugglers relates to new tactics that allow traffickers to leave illicit shipments (e.g., drugs) at high-sea attached to a GPS-enabled radio or satellite buoys. Satellite and radio buoys adapted from the fishing industry are used for this purpose. The application of the electronic system for Electronic Intelligence and Direction Finding allows the detection and localization of these buoys.

Smugglers widely use various kinds of RF communication systems. For example, an abandoned Panga with a $2 million-plus load of marijuana was found in California's Monterey County on the Big Sur coastline. A CB (27 MHz) radio was found on a beach near the Panga boat. The smugglers were arrested in a van. Inside the van, deputies found a CB radio tuned to the same channel as the CB radio found on the beach.

The low-cost and widely used two-way VHF and UHF radios are popular in marine communication. The two most commonly used frequency ranges for two-way radios are VHF (Very High-Frequency at 130-174MHz)**,** and UHF (Ultra High-Frequency at 400-520MHz)

Smugglers also use satellite phones providing reliable communications from any point on Earth and were found on a smuggling boat intercepted by the USCG

Current methods of Electronic Intelligence and Direction Finding provide a natural background for the development of similar methods for the USCG. The current methods are very costly to acquire and operate and require highly qualified operators. The USCG currently employs a radio monitoring system (Rescue 21) that practically covers the whole US coastline. However, this system is expensive (100s of millions and 10s of millions of dollars to operate) and can only detect and localize distress calls. The USCG has equipment with RF directional finding capabilities, where practically all USCG aircraft and helicopters are equipped with direction finders. One of the main systems is the DF-430 Multi-Mission Direction Finder. The DF-430 is specifically designed to receive and interrogate all current international distress frequencies including 121.5 MHz, 243 MHz, 406 MHz, as well as the ARGOS and COSPAS-SARSAT encoded beacon signals.

All current USCG systems are very expensive and require well-trained personnel. This prevents their wide application for illegal boat detection. Their application for USCG needs require development and implementation of software for automated short RF communication signal detection and direction finding. Modern electronics, computers and signal processing methods allow the development of a portable, low-cost RF surveillance system that can be used on various platforms including USCG shore stations, cutters, aircraft, and UAS. Note that our proposed method does not require listening in on calls or messages as it detects the RF spectrum of a signal rather than its contents.

### 2.2.5 Methodology

The primary objective of this project is to provide a proof of concept of RF communication system detection and RF direction finding system which is capable of detecting and localizing communications made by bad actors performing illegal activity in the maritime environment.

Frequency bands were chosen based on an analysis of communication systems (see above) and RF buoys that most likely would be used by a crew of an illegal vessel. These bands include Citizen Band (CB) radio with frequencies around 27 MHz, VHF, UHF two-way radios (150-174 MHz and 421-512 MHz), and Satellite phones (1525-1616 MHz). The Stevens RFSS is designed to provide detection and direction-finding capability within these frequency bands at a lower system cost in comparison to other systems for Electronic Intelligence (ELINT) and direction finding used by the USCG and NAVY.

A method for estimating the detection distances of various communications for parameters of RF sources was developed based on the Line-of-Sight (LOS) and link budget energy evaluation. The link budget method is especially important for a CB radio that can

propagate over the horizon and is using spectrum range that is much less occupied than other frequencies used for communication. The estimation of detection distances has been conducted based on known experiments of RF wave propagation above the sea and RF ambient noise measurements in various areas of the USA. The initial detection system was built based on a low-cost Software Defined Radio (SDR). Tests conducted at Padre Island confirmed the feasibility of this approach for reliable detection of communication systems at sea. In this experiment, the detection distances in VHF band were about 13 km.

In this project, we are investigating various opportunities for the development of a radio monitoring system that can detect and localize different RF emitters on boats and emitters on the shore (cellular and satellite phones, maritime communication systems, two-way radios, CB radio, GPS trackers using satellite or radio communications, etc.). Several setups that were developed and investigated include:

- A low-cost amateur radio direction finder, the Stealth DF2020, with a 4-antenna switch useful in the VHF band was purchased and tested in laboratory conditions. It has shown limited usability for surveillance, however it provides reasonable performance as a single-channel direction finder.

- A multifrequency setup for detection of RF signals radiated from a small boat was built and tested in the Padre Island, TX area. The RFSS sensor setup consisted of three separate raw-data RF monitoring systems and a single wideband analyzer system. Three specific bands suggested by the USCG were investigated, each with their own antenna deployed on the roof: CB Radio (27 MHz), VHF (144 to 148 MHz), UHF (450 to 470 MHz).

- A portable system for RF signal recording from small Unmanned Aerial Systems (UAS) was developed and tested. This system is based on a Software Defined Radio installed on a UAS. This system can be used on a small tethered UAS to significantly extend the system detection range and operation capacity.

- Stevens developed and built a radio direction finder (RDF) based on a software-defined radio (SDR) and pseudo-Doppler principles of direction-finding at its center, along with software that facilitates processing, display, and integration with mapping systems. The RFSS is capable of automated multi-channel direction finding in the frequency bands of interest and is equipped with a user-friendly interface built using low-cost commercial off-the-shelf (COTS) components. Software for the angle of arrival (AoA) finding was developed for this system. It includes a graphical user interface (GUI) for monitoring radio frequency spectrum in real-time and directions towards received signals. An RDF antenna switching system with 8 inputs for the CB band was assembled and tested in a mobile installation on a van roof. This system was investigated for detection and direction finding of RF signals radiated from a boat in the Hudson River.

### 2.2.6 Project Milestones and Performance Metrics

The project deliverables are shown in Table 1.

*Table.1. The planned and modified project deliverables.*

| No. | Initial Deliverable | Deliverable completion and modification |
|---|---|---|
| 1 | Building several set-ups to prove the concept of the RF surveillance system for the USCG applications in monitoring boat illegal activity. | Complete. In addition, we conducted the sea field test in Padre Island that was not in the initial work plan. |
| 2 | Investigating a laboratory set-up and one at sea at the NJ shore. Finding system parameters and demonstrating the applicability of the suggested solution for implementation in USCG operations. | Due to COVID-19 restrictions the tests were not conducted at the NJ shore. The field test in Padre Island and a number of the laboratory tests were conducted instead. |
| 3 | Writing a final report that describes the test and test setups in full, including all research and analyses performed prior to the tests, the testing procedures, data collected, and findings. The report will also include recommendations for building a system optimized for USCG applications. | The final report was prepared and submitted in September 2020. Additional materials about the development of Stevens RFFS field test results are included in the current annual report. |

The project milestones and their completion are presented in Table 2.

*Table 2. The protect milestones and their completion.*

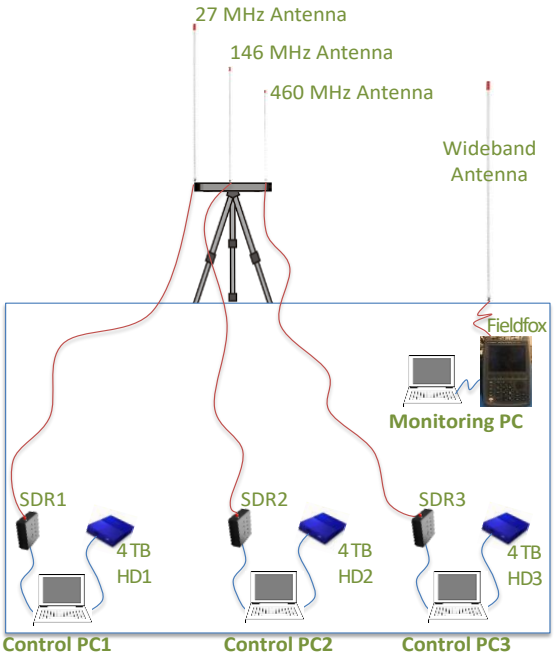
| No. | Planned Milestone | Planned Time Frame | Completion |
|---|---|---|---|
| M1 | Kick-off meeting to discuss project plan, objectives, and outcomes. | October 2019 | Complete. |
| M2 | Experimental RF surveillance setups for land and ship application tested in the lab. | February 2020 | Complete. In addition, a Padre Island field test was conducted that was not included in the work plan. |
| M3 | An RFSS test platform using laptop computer as main processor has been designed. Simulation of expected signals developed to aid in processing pipeline and algorithm, design while forced outside of the lab. | May 2020 | Complete. |
| M4 | Perform laboratory testing of the RFSS test platform upon regaining access to facilities. | August 2020 | Complete. The system building has been completed and |

| | | | |
|---|---|---|---|
| | The goal is to validate system design and detection methodology. | | laboratory tests have been conducted. . |
| M5 | Create a set of requirements for compressing the RFSS into an integrated SDR platform that is capable of being installed on a UAS and determine if such a design is feasible. | Septemb er 2020 | Set of requirements for compressing the RFSS into an integrated SDR platform was created. |

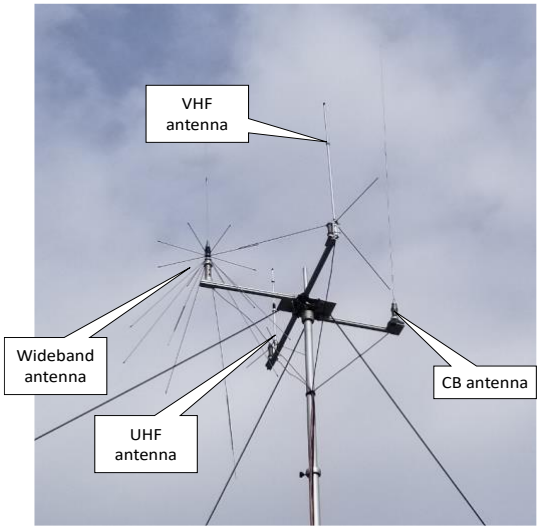
The following performance metrics were completed:

**RFSS setup tested at sea at Padre Island**

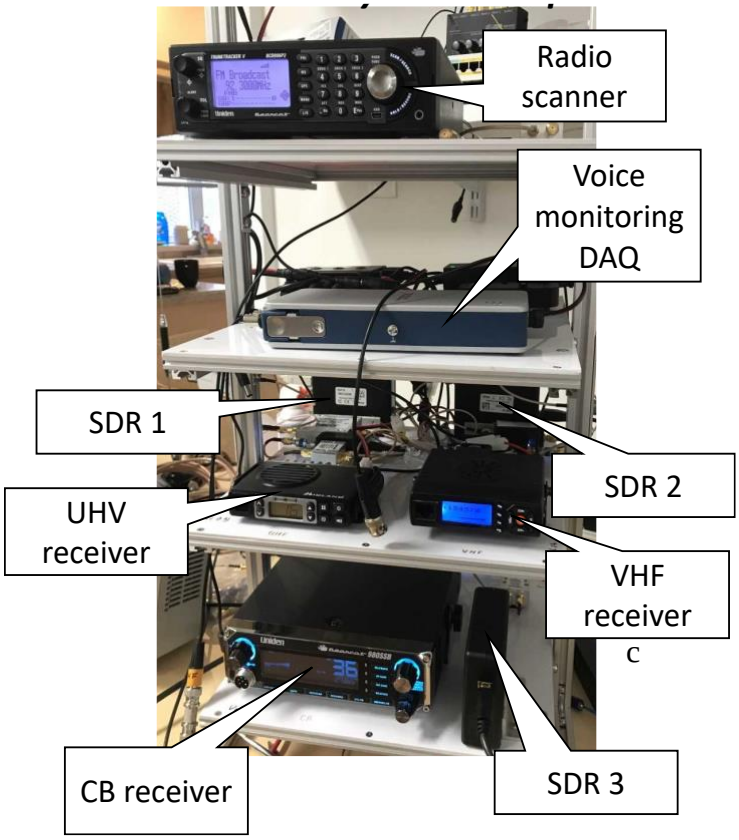
The picture of the sea test setup for detection of RF signals radiated from a small boat is shown in Figure 1. The RFSS sensor setup consisted of three separate raw-data RF monitoring systems and a single wideband analyzer system. Each raw-data RF monitoring system recorded 14-Bit I/Q RF data at a rate of 10 MHz. The wideband analyzer consisted of a Keysight FieldFox, wideband antenna and monitoring PC. Three specific bands were investigated, each with their own antenna deployed on the roof: CB Radio (27 MHz), VHF (144 to 148 MHz), UHF (450 to 470 MHz).




a




b




c

c

*Figure 1. The RF signal receiving setup used in the Padre Island field test: a) Schematic of the shore-based RF receivers' setup; b) Antenna system; c) Picture of the equipment.*

**Flying RFSS installed on drone**

In addition to the main task of the project, Stevens developed and built a lightweight and mobile system for RF signal recording that can be conducted from a UAS. In this work, the UAS used was donated to Stevens by a local pilot. This system, dubbed the SDR for Experimental Aerial Mounting (SDREAM) Test Bed, is small enough to be handheld or even attached to a drone in order to facilitate multiple GPS-tagged RF signals recording in a single UAS drone flight. The picture of the RFSS SDREAM attached to the drone is shown in Figure 2.

*Figure 2. SDR for aerial recording of RF signals installed on a Stevens DJI S1000 drone.*

The SDREAM Test Bed's SDR can operate as a full duplex, multiband radio. The radio has a total operational bandwidth ranging from 70 MHz to 6 GHz, allowing it to function across ISM frequency bands of interest (915 MHz, 2.4 GHz, and 5.8 GHz), as well as many other common communication channels including but not limited to UHF, VHF, 700, Cellular, AWS, PCS, 2600, and L-Band. The DJI S1000 aircraft was considered a mounting platform. In order to incorporate the SDREAM Test Bed onto the DJI S1000 a special harness was also 3D printed to facilitate a natural integration between the two systems. As shown in Figure 2 the final construction of the system was able to seamlessly attach to the DJI aircraft. COVID restrictions did not allow us to conduct flight tests of the developed system. SDREAM is ready for tests that can be conducted when COVID restrictions are removed.

**RFSS prototype with direction finding capabilities**

We built the automated Radio Frequency Surveillance System that has a radio direction finder based on a software-defined radio and pseudo-doppler principles of direction-finding at its center, along with software that facilitates processing, display, and integration with mapping systems. It is capable of automated multi-channel direction finding in the frequency bands of interest, equipped with a user-friendly interface built using low-cost commercial off-the-shelf components. The software and the hardware for the initial system

were built for 27 MHz CB radio. The schema of the system and its picture are shown in Figure 3.

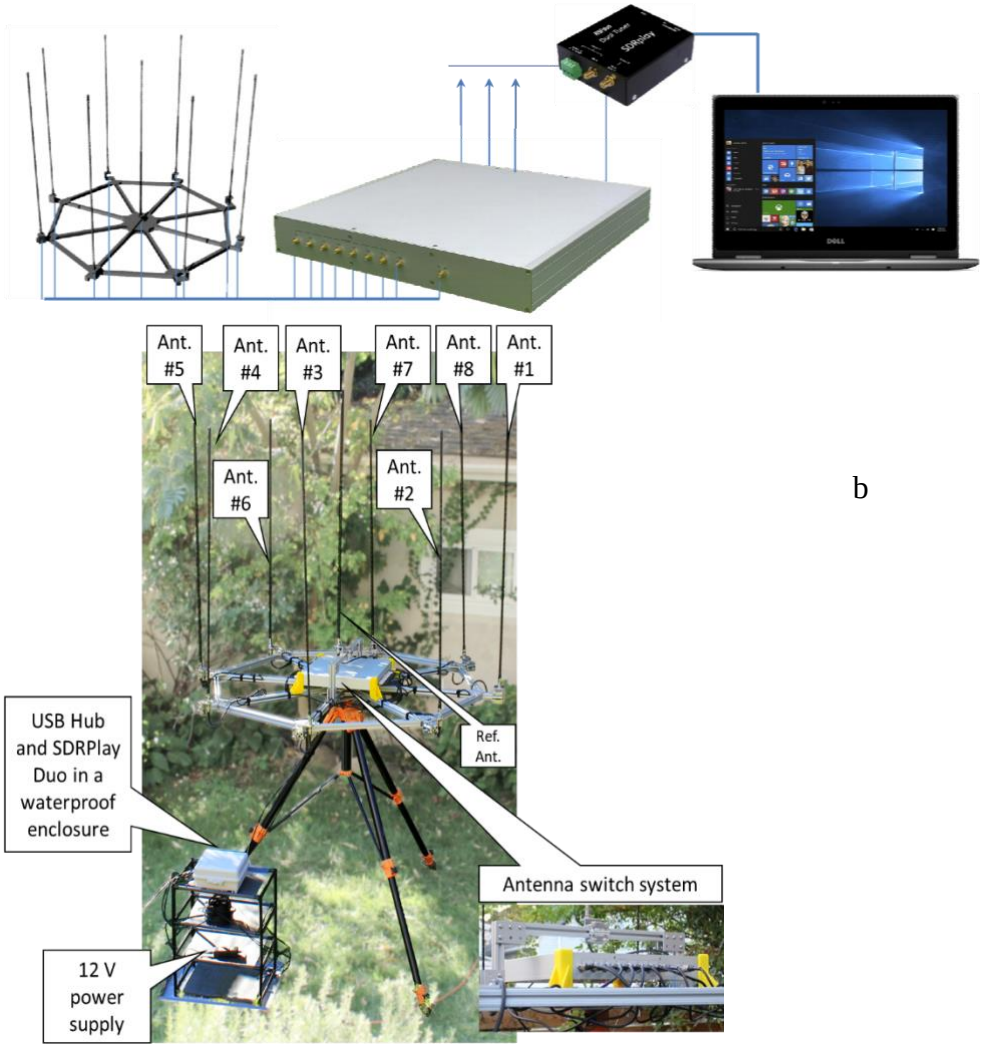



*Figure 3. Schema of RFSS CB band radio direction finding system (a) and its picture (b).*

Software for the angle of arrival (AoA) finding was developed, including a graphical user interface (GUI) for monitoring radio frequency spectrum in real-time and directions towards received signals. The software was tested using simulated RF spectrum data. Additional drivers for interfacing a low-cost dual-channel SDRPlay RSPDuo SDR were developed, along with communication protocols and formats for processed data allowing to transfer data from the low-level software to the GUI and for storage of logs on a disk.

**Boat-based system of transmitters**

The RFSS target signal sources were to be deployed onto a target surface vessel as shown in Figure 4. Each radio was tuned to a target radio band: Uniden Bearcat 980SSB CB Radio (27 MHz), Zastone 218 Mobile Car Radio (VHF, 146 MHz), Midland 5-Watt

GMRS MicroMobile Two-Way Radio (UHF, 460 MHz). All equipment was powered using high-capacity 12 V batteries. Each radio was modified to transmit regularly. Transmissions were made according to the following scheme: 2 seconds of transmission on CB band, 2 seconds of transmission in the VHF band, 2 seconds of transmission in the UHF band, then 8 seconds of silence. CB transmissions were made on channel 28 (27.285 MHz) with 400 Hz AM modulation, VHF transmissions were made on MURS channel 4 (154.57 MHz) with 400 Hz FM narrowband modulation, and UHF transmissions were made on channel 16 (462.575 MHz) with 400 Hz FM narrowband modulation.

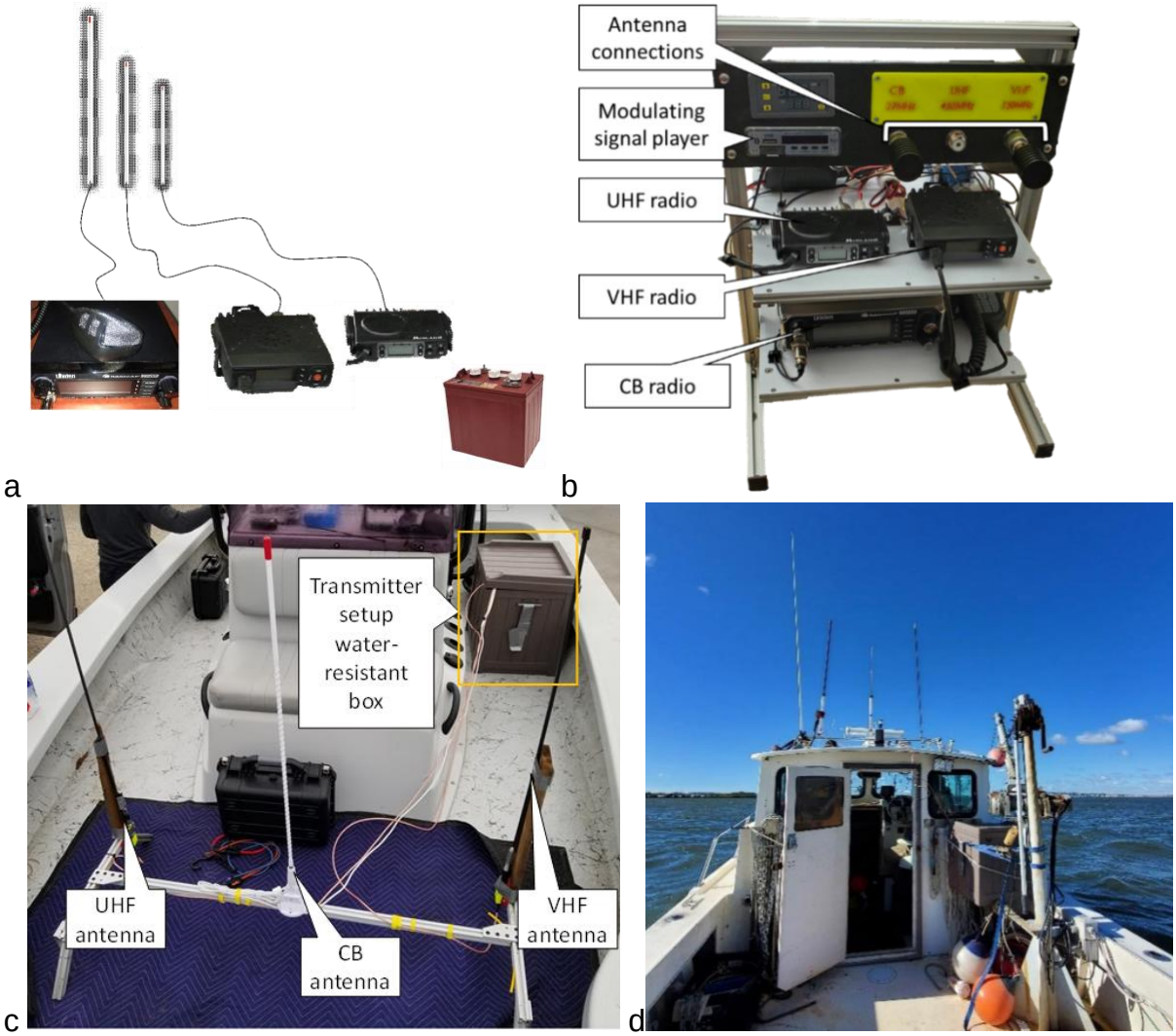



*Figure.4. Radio transmitter setup: a -schematic representation, b - assembled, c - deployed on the boat. d – Antennas mounted to the roof of the vessel.*

### 2.2.7 Transition Plan

The resulting research and project report generated from this endeavor include a prototype RF surveillance system optimized for USCG applications. The applicability of such an RF surveillance system, its practical limitations, and its ease of operation are being discussed

with the USCG to determine transition requirements and tasks at the end of the project. A user-friendly prototype of an optimal, low-cost system can be built and tested in a future phase of the project. The proposed system should deliver proven surveillance capabilities of illegal vessels and their accomplices, providing a unique opportunity to enhance the USCG mission capabilities via persistent surveillance of ports, coastal approaches, maritime sanctuaries, and smuggling activities that will reduce operational costs without degrading mission performance.

The cost of the RFSS array components is $4000, and the cost of the central computer is $1,500. The same cost estimation is similar for different frequency ranges. We expect that all four frequency ranges of interest (CB Radio, VHF, UHF, and Satellite phone) can be covered by 4 systems. The total component cost for covering these four bands is $17,500.

During the work, Stevens researchers found several novel technical solutions in the RFSS design and signal processing that could be the basis for patent applications. Provisional application(s) could be filed in case this work continues.

If the system provides the functions and performance needed by the USCG, we will seek a company to license and manufacture the RFSS. Our priority will be given to companies that have been selling maritime products to the USCG. Then the existing USCG acquisition process can be used to purchase this system. During the preparation stage for system manufacturing, we plan to prepare all system documentation as well as training materials as we have done in the past for similar systems and provide these as part of a transition process. These will include the following: principles of operation, system architecture, system specifications, system configuration and revision history, Level 3 drawing package, Interface Control Documents (ICDs), component supplier noted on drawings, set-up/tear down manual, permission to operate, operator manual, maintenance and spares requirements for 3 years of operation. The software will be prepared as an executable package with installation and user manuals for the USCG to evaluate.

### 2.2.8 Stakeholder Engagement

The USCG is the primary stakeholder for this work. Other prospective stakeholder organizations may include: NAVY, Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Federal Emergency Management Agency (FEMA), the U.S. Secret Service (USSS), the Domestic Nuclear Defense Office (DNDO), the Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), Department of Defense (DoD), SOCOM, DARPA, NOAA, DOT Office of Maritime Security, Alliance for Coastal Technologies – ACT, and the National Maritime Security Advisory Committee (NMSAC).

The need of the USCG for the suggested work has been articulated by USCG Sector Corpus Christi in discussions with researchers from Stevens. Stevens team visited Corpus Christi in February 2017, October 2019 and in January 2020. We gained first-hand insight into the terrain where illegal drug operations often occur in order to propose technical solutions to improve drug interdiction operations and illegal fishing interdiction. We also

learned about the environment limitations, including access to the beach area, protected species, available locations for installation and communications, etc. The MSC team has actively engaged the USCG stakeholders in this project. The POC from the USCG HQ was engaged throughout the planning and execution of this project and acted as the liaison with other USCG personnel. The results of the work are actively being discussed and shared with USCG Project Champions.

### 2.2.9 Programmatic Risks

The project has successfully completed. The final report has been submitted to DHS.

We described some risks that can prevent or limit future applications of RFSS by USCG. These risks included:

- Main risk is related to the awareness of illegal boat crew that RF surveillance may be conducted. They may limit RF communications and use short messages for communication. This risk could be reduced by developing signal processing methods for automated RF signal interdiction and direction finding of short communications.

- Another risk may be connected with the limited sensitivity of the developed low-cost Electronic Intelligence and Direction-Finding setups. We would have worked on mitigating this risk by adjusting the RF antennas, using specific antennas for various frequency bands, improving preamplifiers and signal processing algorithms.

### 2.2.10 Progress

The progress against each milestone outcome is shown in Table 1. All planned items have been reached, but with some delay due to restrictions imposed by the COVID pandemic. The finalization of the RFSS system prototype with DF capabilities and the planned field tests at the NJ shore were conducted after the end of the project in the beginning of 2021.

### 2.2.11 Unanticipated Problems

Due to the COVID 19 pandemic, we had to adjust our timeline and test plans. We concentrated our efforts on the mathematical modelling, software development and laboratory tests that allow successful completion of the project. The final field tests were conducted with minor delays.

### 2.2.12 Information supported by data

The suggested RFSS can effectively improve surveillance, detection, classification, and identification of illegal vessels, their accomplices on the land or at sea and RF buoys used for location of contraband left at sea. For this project, our aim was to show a proof of concept of a simple low-cost RF surveillance system that can be used by the USCG to aid them with the detection of illegal activities from vessels.

The sea field test conducted in Padre Island demonstrated the reliable detection of RF signal used for two-way communications at distances of 13 km. We developed novel algorithms for RF signal detection distance prediction that can be used for the estimation of the system performance in USCG operational conditions.

The RFSS system prototype with direction finding capabilities (see Figure 3) is the main output of the project. All parameters describing the RFSS performance were investigated in the laboratory, sea field tests and field test in the Hudson River, confirming the predicted laboratory measured performance parameters. Work for RFSS preparation for transition may be conducted in a future phase of this work.

## 2.3 Safety and Security of Remote Bridge Operations Project

PI: Randall Sandone, University of Illinois at Urbana Champaign
Project Period: October 2019 - June 2021
Budget: $242,778

### 2.3.1 Changes from Initial Work Plan

Our project developed and published an annotated Risk Management Plan based on the NIST Risk Management Framework that can be used by USCG as a foundation for policy and guidelines of the domain. This document is available for release to any interested party.

In addition, we developed and published a proposed NIST Cybersecurity Framework (CSF) Profile for Remote Bridge Operations. This document is also available for release to any interested party. The NIST CSF Profile for Remote Bridge Operations has been ingested and operationalized in the DHS/CIRI-developed Cyber Secure Dashboard and made commercially available as a Software-as-a-Service (SaaS) offering or as an on-premise solution.

Because of COVID 19 travel restrictions at the conclusion of the project, we had unspent travel funds. To enhance the profile and Cyber Secure Dashboard we reallocated the funds to bring the Cyber Secure Dashboard up to NIST SP 800-53 Rev 5, which is the foundation for the Remotely Operated Bridge profile. The NIST SP 800-53 Rev is only linked to the Remote Bridges standard.

### 2.3.2 Objective

The objective of this project is to enhance the security and resilience of the nation’s movable bridge infrastructure by assisting the USCG in developing a sound, voluntary, standardized risk management regime to help guide bridge owners and operators in the implementation and maintenance of remote bridge operations in a more secure and resilient manner.

### 2.3.3 Baseline

Current and legacy movable bridges are operated by human operators at the bridge site. As the category name implies, remote bridges are operated remotely through commands delivered via information and communications technologies (ICT) to remotely signal the actuators and other components that operate the bridge.

The current baseline concept of operations for cyber risk assessment and management of remote bridges is essentially BYOP (bring-your-own-policy) and BYOS (bring-your-own-standard). Each bridge owner or operator addresses cybersecurity and cyber risk management in a bespoke manner. There is no mandated or recognized voluntary cybersecurity standard, policy, or framework representing industry/domain best practices. Consequently, the various remote bridges stakeholders — the bridge owners & operators; maritime, land and rail shipping companies; regulators; insurance carriers; municipalities, etc. — are unable to accurately assess the relative risk of various remote bridge designs and/or operational procedures and unable to accurately assess the relative cyber risk management maturity of owners/operators that are operating remote bridges. Most importantly, without sound, standardized cybersecurity standards and risk management processes in place, those responsible for public safety and the safety of waterways and highways are unable to accurately assess the safety of movable bridges that have transitioned to cyber-operated remote operations and/or the cybersecurity maturity of their operators.

This project has delivered sound cybersecurity standards and risk assessment, and management processes and procedures, for voluntary adoption by remote bridge stakeholders to directly address the current deficiencies addressed above. These proposed standards and procedures are based on sound and thorough research into the potential vulnerabilities in remote bridge architectures and the cybersecurity and operational processes of the operators of those bridges. The framework for the proposed standards and procedures and the security controls required to comply with the standards are based entirely on national standards issued by the National Institute for Standards and Technology (specifically the NIST Risk Management Framework, NIST Cyber Security Framework and NIST SP800-53).

### 2.3.4 Methodology

With the support of USCG, and the stakeholders listed in Section 2.3.7 below, this project conducted a thorough analysis of remote bridge operational architectures to determine best available practices and required security considerations for remote bridge operations. Our analysis considered analogous operations in distributed cyber-physical systems and identified practices and protocols from other sectors such as pipeline supervisory control and data acquisition (SCADA) systems. Informed by this analysis, the project developed and published an annotated Risk Management Plan based on the NIST Risk Management Framework that can be used by USCG as a foundation for policy and guidelines of the domain.

This project also developed and published a Remote Bridge Operations Profile based on the NIST Cybersecurity Framework (CSF). Lastly, the project implemented the Remote Bridge Operations Profile in the CIRI/DHS-developed Cyber Secure Dashboard for use by the remote bridge operations community to guide and manage conformance to the Profile.

### 2.3.5 Milestones and Performance Metrics

| Milestone | Description | Completion Date |
|---|---|---|
| 1 | Kickoff Meeting (All) | September 26, 2019 |
| 2 | Landscape & Scoping Study | April 24, 2020 |
| | 2a. Bridge Inventory | April 24, 2020 |
| | 2b. Systems Inventory | April 24, 2020 |
| | 2c. Regulatory Review | April 24, 2020 |
| 3 | Taxonomy | August 31, 2020 |
| 4 | Site Visits (Moved to remote b/c of COVID 19 travel restrictions). | June 30, 2020 |
| 5 | RMF | September 30, 2020 |
| | 5a. Best Practices | September 30, 2020 |
| | 5b. Interviews and Sight Visits | September 30, 2020 |
| | 5c. Draft RMF and tool development | September 30, 2020 |

| Deliverable | Description | Completion Date |
|---|---|---|
| 1 | Literature Review | January 2020 |
| 2 | Landscape & Scoping Report | April 2020 |
| 3 | Taxonomy Document | August 2020 |
| 4 | Completion of Draft NIST RMF and CSF Profile | September 2020 |
| 5 | Completion of cyber dashboard implementing the developed NIST CSF profile | September 2020 |

All identified deliverables are complete and have been submitted to our sponsor and USCG.

| # | Key Performance Metrics (KPM) | Baseline | |
|---|---|---|---|
| | | Threshold* | Objective* |
| KPM #1 | Site visits with operators (Remote) | 1 | 5 |

| | | | |
|---|---|---|---|
| KPM #2 | Beta RMF Profile incorporates stakeholder feedback on Alpha profile | Pass | Pass |
| KPM #3 | Pilot test of dashboard | 3 organizations | 5 |

* This table represents the key metrics we established before the project began to provide the research team with targets for key success metrics of the research project. "Threshold" refers to the minimum target. "Objective" refers to the goal we planned to achieve for the particular activity. In the case of KPM#1, we achieved the "Objective" of at least 5 remote engagements to gather data regarding the remote bridge architectures and the operational procedures followed by remote bridge operators. KPM#2 sets the target of ensuring that we incorporated stakeholder feedback regarding the annotated Risk Management Framework on a simple PASS/FAIL scale. We did indeed secure feedback so we achieved a PASS. KPM#3 represented a target for pilot testing the Remote Bridge Profile with 3 – 5 organizations. Given the delays occasioned by the pandemic, we were unable to get the Profile integrated into the Dashboard in time to conduct pilot tests prior to the end of the period of performance. Although a pilot test was a goal of the research team, it was not a formal milestone or deliverable. Accordingly, we believe that the project was a success. In spite of the disruption caused by the pandemic and lockdown the team was able to secure valuable stakeholder feedback which informed the development and publishing of an Annotated Risk Management Framework (RMF) document; the development and publishing of a NIST CSF-base Remote Bridge Operations Profile; and the integration of that profile into the DHS-funded Cyber Secure Dashboard – all formal requirements of the project grant.

### 2.3.6 Transition Considerations

The project has transitioned to the public domain an annotated Risk Management Plan template and the Remote Bridge Operations CSF Profile, based on the NIST CSF. Both standards are complete, and the CSF Profile has been embedded in the Cyber Secure Dashboard.

The Remote Bridge Operations Profile implemented in the CIRI/DHS-developed Cyber Secure Dashboard will be made available on a voluntary basis for use by the remote bridge operations community via commercial license subscription to guide and manage conformance to the Profile.

### 2.3.7 Stakeholder Engagement

| Stakeholders | Role | Interaction date | Outcome |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Janet St. John<br>AAR, | Director, Cyber Security Association of American Railroads | 6 March 2020<br>31 March 2020<br>15 May 2020<br>22 May 2020<br>23 June 2020<br>19 August 2020<br>2 September 2020<br>4 November 2020 | Janet (AAR): Initial discussion to gauge interest, AAR is interested and willing to work with us. AAR attempted to engage with our project, however, due to COVID, schedule in flux, and restricted staff they were unable to follow through with the engagement. Janet St. John did continue her engagement and provided feedback and input on the draft RMF and CSF. |
| Jeff Hieb | Port Security Specialist, Milwaukee | 13 March 2020 | Jeff agreed to develop a list of key contacts within the City of Milwaukee and to help arrange and coordinate site visits either physical or virtual. |
| Kamal Elnahal, Ph.D., P.E. | Chief, Bridge Operations and Engineering Division (CG-BRG-1), Bridge Program, U.S. Coast Guard | 30 Jan 2020<br>30 Apr 2020<br>23 Jun 2020<br>17 Jul 2020<br>24 Jul 2020<br>20 Aug 2020<br>28 Sept 2020<br>13 Oct 2020<br>2 Nov 2020<br>4 Nov 2020<br>21 Jan 2021<br>27 Jan 2021<br>29 Jan 2021<br>26 Mar 2021<br>29 Mar 2021 | Dr. Elnahal received regular status updates throughout the project. His input was solicited regarding all final deliverables. We worked with Dr. Elnahal to coordinate the final USCG brief. |

| | | | |
|---|---|---|---|
| | | 28 Apr 2021 | |
| Christopher Barkan, Ph.D. | George Krambles Director, Rail Transportation & Engineering Center, UIUC | 7 May 2020 | Initial discussion to map out engagement with RR owners and operators and rail industry associations. |
| Brian Wisniewski | NASA office of Cybersecurity Services, Operation Manager | 5 January 2021<br>11 January 2021 | Provided feedback and input on the draft RMF and CSF |
| Jim Blevins | Cooper Tire, Cyber Security Director | 16 November 2020 | Provided input on the draft RMF and CSF |
| Lisa Young | Axio, Cyber Risk Engineering | 27 October 2020 | Provided preliminary recommendations addressing the approach and scope of the RMF and CSF |
| Drew Tucci | CAPT. USCG (Ret) Maritime Consulting | 6 January 2021 | Provided feedback and input on the draft RMF and CSF |

### 2.3.8 Potential Programmatic Risks

This project is complete, and all outputs have been delivered to the sponsor. The MSC research team from CIRI will continue to promote the Remotely Operated Bridge CSF Profile and the Annotated RMF.

### 2.3.9 Unanticipated Problems

Due to the COVID-19 travel restriction, we were unable to deliver a taxonomy document according to our project timeline. In response to this unanticipated problem, we moved to a remote engagement with bridge owners and operators to gather the architecture data needed. We pivoted the project's engagement strategy from a smaller face-to-face sample

size to engaging with the Association of American Railroads members to collect pertinent data. Our team created a survey that was distributed on our behalf to AAR.

### 2.3.10 Information Supported by Data

As stated above, there is no domain-wide cybersecurity standard or standardized cyber risk assessment and management process or even a published compendium of best practices being applied to the transition to remote bridge operations. Bridge owners and operators are individually left to develop, implement, and maintain a cybersecurity posture and risk management process on their own. This lack of standards makes it difficult to assess the relative underwriting risk posed by a particular remote bridge operator, which in turn impedes the development of a robust and mature market for cyber insurance in this domain. Likewise, those federal, state, and local government agencies with oversight responsibility for safety of rail, highway, and maritime transportation have inadequate reference points for assessing the safety and security of remote bridge operations.

The outcomes from this project directly addressed these issues by delivering proposed cybersecurity standards and best practices that are in compliance with NIST standards and guidelines. Domain-wide adoption of such standards and best practices would establish the foundation for assessing the relative risk of specific remote bridge operations (and the owners and operators of those bridges) based on their level of compliance and adherence to those standards and best practices. This would facilitate the maturation of the cyber insurance market in the domain — resulting in more available and more affordable policies — lowering costs and reducing financial risk to bridge owners and operators. Likewise, adoption of sound cybersecurity and risk management standards and best practices would ease the burden on regulators by providing sound metrics upon which to base policy and oversight.

## 2.4 VTS Radar for Small Vessel Detection

PI: Dr. Hugh Roarty, Rutgers University
Project Period: January 2020 - June 2021
Budget: $204,973

### 2.4.1 Changes from Initial Workplan

The COVID-19 pandemic prevented the MSC research team from completing all of the in-person visits to the Vessel Traffic Service (VTS) centers as originally outlined in the work plan. With the help of Lt. Eric Romero, USCG Office of Shore Forces, we were able to conduct phone interviews with the remaining VTS centers to gather requirements for radar and other sensors within the VTS operations.

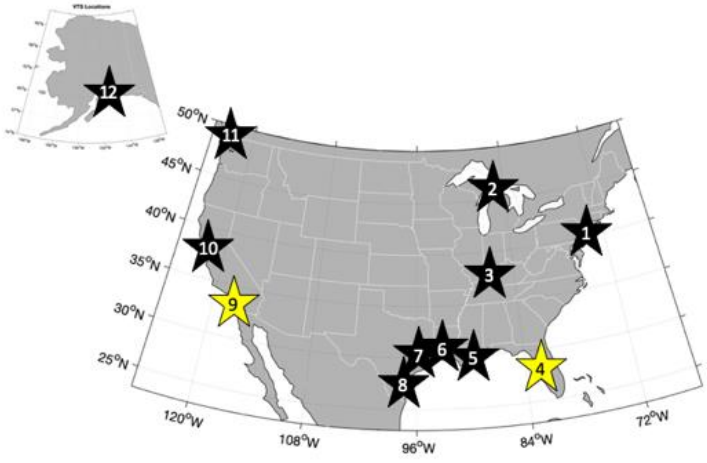
### 2.4.2 Objective

Rutgers University was funded through the Maritime Security Center to develop a needs analysis for United States Coast Guard Vessel Traffic Service (VTS) centers with respect to radar remote sensing for small vessel detection and other applications.

### 2.4.3 Baseline

There are 12 VTS centers across the United States, 10 of them are managed by the Coast Guard and two are cooperatives where the Coast Guard provides watchstanders. The location of the VTS centers is shown in Figure 1. Eight of the top ten ports in the US are covered by a VTS [1]. The 12 VTS in this study provide situational awareness for 3,000 vessels per day so having the proper sensors to collect and distribute that information is essential.

| No. | Vessel Traffic Service |
|---|---|
| **1** | New York, NY |
| **2** | St. Mary's River |
| **3** | Louisville, KY |
| **4** | Tampa, FL |
| **5** | Lower Mississippi River, LA |
| **6** | Berwick Bay, LA |
| **7** | Port Arthur, TX |
| **8** | Houston/Galveston, TX |
| **9** | Los Angeles-Long Beach, CA |
| **10** | San Francisco, CA |
| **11** | Puget Sound, WA |
| **12** | Prince William Sound, AK |




The Coast Guard is currently developing plans for its next generation Vessel Traffic Service (USCG Capability Analysis Report for Vessel Traffic Service, 2019). The Capability Analysis Report (CAR) [2] identified 12 capability gaps within the VTS, 2 pertaining to radar. The first being lack of sufficient resolution from the radar systems, the second being the inability to properly display the desired resolution in the Port and Waterways Safety System (PAWSS). One of the major challenges that the

*Figure 1: Map of the US showing locations of the Vessel Traffic Service Centers. The two stars in yellow indicate VTS that are run as a cooperative.*

CG is facing within VTS right now is the obsolescence sustainment of their radar systems. The two radar systems utilized within the VTS are the Terma Scanter 2000 (end of life 2027) and Furuno FAR-3000 (end of life 2015).

This work plan utilized all the information obtained from the previous MSC radar project [3], especially to identify radar vendors. These vendors received a request for information that was developed in this project. The main objective was to gather USCG requirements to develop the RFI, analyze responses, and make recommendations to seek potential new VTS radars that are capable of detecting small vessels with acceptable performance to the USCG VTS mission. The focus was to find radars that will replace existing radars and help the USCG identify radars that provide the best performance for detecting small vessels and other non-reporting vessels.

We have identified the VTS mission needs statement for radar and other sensors:

The system surveillance capability should have sufficient resolution to detect, classify, and identify vessels and objects that may disrupt marine traffic or become hazards to navigational safety in both day and night situations, as well as in low visibility environments. The sensors should be connected to their local hub via an infrastructure with adequate bandwidth (e.g., potentially leveraging 5G, fiber optics, or other high-speed networking technology) for further connection to a networked system. There should be multiple levels of sensing capabilities, such as radars and cameras, tailored to the unique geographical layout and specific mission needs of each VTS, which will be adequate to provide coverage throughout each VTS area of responsibility (AOR) as defined in 33 CFR 161. The display system should be capable of transmitting and receiving the signals with minimal loss of fidelity and should have a configurable display.

This research project will consist of the tasks outlined in Table 1. This report summarizes work in support of Tasks 1-7.

*Table 1: List of tasks defined for this research study.*

| No. | Task | Time Frame | Status |
|---|---|---|---|
| T1 | Visit USCG VTS Centers | Months 1 to 2 | Complete |
| T2 | Document requirements for small vessel detection | Month 1 to 6 | Complete |
| T3 | Develop market survey of existing radars | Month 1 to 8 | Complete |
| T4 | Develop request for information (RFI) and release it | Month 6 to 8 | Complete |
| T5 | Analyze received RFI responses | Month 8 to 10 | Complete |
| T6 | Tabulate RFI responses and provide recommendations | Month 9 to 11 | Complete |
| T7 | Final report | Month 12 | Complete |

### 2.4.4 Methodology

**Kickoff Meeting**

The MSC research team started the project with a kickoff meeting at Coast Guard Headquarters. Representatives from CG-741 Office of Shore Forces (Lt. Eric Romero, Lt.

Michael Griffis), CG-761 Office of Sensor Capabilities (Mr. Brian Page), CG-771 Office of Requirements (LCDR Russell Hall), CG-681 C4IT (Lt. Matthew Lynne) and CG-NAV (Mr. Darin Mathis). Dr. Roarty introduced his project, then there was an open discussion on the project.

Each VTS has its own capability feeds and there's no interconnection between them. But there is standardization across the VTS centers in terms of sensors and components. Coast Guard is currently in the pre-acquisition phase for next generation VTS. They've built the case for recapitalizing and redesigning the system.

The Coast Guard is solution agnostic. They are not bound to any one vendor. They are open to sensors other than radar, thermal, optical, signals intelligence. There is a big emphasis in the Coast Guard for innovation and leveraging new technologies. The Coast Guard would like to perform an analysis of alternatives for VTS sensors that includes examination of cost, user effectiveness and mission effectiveness. The Coast Guard would like to see this report shed light on VTS mission needs that the Coast Guard is unaware of.

There was a discussion of radar particulars. Does the CG have the proper support infrastructure to maintain these radars? The digitization of the radar needs improvement. The analog signal looks good, the digital picture is poor. The need for radar within the VTS is real. Small vessel detection is what the VTS centers need. VTS Seattle needs to be able to manage the large number of tribal fishing boat while VTS San Francisco has a large recreational boating community that is a challenge. All of these vessels fall under the SOLAS class vessels (300 gross tons and above) that most of the VTS centers are focused on.

The team then laid out a series of dates where we would travel to certain VTS centers to talk with the directors, watchstanders, Electronics Material Officer (EMO) about the needs for radar within the VTS.

**VTS Visits**

The Rutgers team developed a questionnaire that was delivered to a VTS center before the visit. We planned to visit each of the VTS centers in person, but the COVID-19 pandemic prevented us from travelling. So, the remainder of the interviews were conducted on the phone. The dates for the interviews with the VTS centers are presented in Table 2.

*Table 2: Dates and modes for interviews with VTS centers on radar needs.*

| No. | Vessel Traffic Service | Interview Date | Mode |
|---|---|---|---|
| **1** | New York, NY | February 6, 2020 | In person |
| **2** | St. Mary's River | | |
| **3** | Louisville, KY | February 26, 2020 | In person |
| **4** | Tampa, FL | | |
| **5** | Lower Mississippi River, LA | April 6, 2020 | Phone |

| | | | |
|---|---|---|---|
| **6** | Berwick Bay, LA | April 28, 2020 | Phone |
| **7** | Port Arthur, TX | March 13, 2020 | In person |
| **8** | Houston/Galveston, TX | March 13, 2020 | In person |
| **9** | Los Angeles-Long Beach, CA | June 24 & July 28, 2020 | Phone |
| **10** | San Francisco, CA | April 22, 2020 | Phone |
| **11** | Puget Sound, WA | April 14, 2020 | Phone |
| **12** | Prince William Sound, AK | | |

The team received valuable input from each of the VTS centers. We also conducted two interviews with personnel from the C5i Service Center on February 19, 2020 and June 3, 2020. A complete documentation of the VTS input is provided in the final report. The team received two pieces of critical information from the interviews. The first piece of information was the need for radar within the VTS as discussed with VTS New York (Figure 2.) This outlined the capability requirements that radar currently delivers within the VTS NY. We will look to see how new generations of radar or other sensors (camera, infrared, laser, etc.) can meet the same requirements. The second piece of information came from VTS Port Arthur (Figure 3). This included a screenshot from the PAWSS display showing a vessel moving south through the VTS. The AIS information is only displayed as a dot on the map. The radar provides the bounds of the vessel within the channel which the operators have communicated is essential for the management of the traffic.

**Thomas, Ashly L LT**

**Subject:** VTS NY Radar Uses/Future Needs

---

The requirements for commercial vessels to have a properly installed AIS shifted the primary means of VRMS and VTS user tracking from RADAR to AIS. However, VTS NY still utilizes RADAR as a normal part of the job. Anchorage monitoring and tracking of Non-AIS VMRS Users are the more common uses of RADAR in daily operations. RADAR is crucial in small vessels tracking, mission support (e.g., Security Zone Violations, and SAR) and breakaways where AIS is not available or may be unreliable in detection of developing situations.

1. Anchorages:
-VTS NY leverages control of over 9 Federal anchorages that are used continuously by the commercial vessels (CFR authority); to best manage these anchorages and maximize the number of vessels simultaneously, we assign the vessels specific spots within the anchorage. To ensure that the vessels ultimately anchor in these spots, we rely heavily on the radar return to ensure we tell the pilot when to drop anchor so as to not impede the adjacent vessels: as the vessels anchor, our operators are guiding them into the center of the spot allocated for them.
-On a yearly basis, we have over 6825 vessels using the anchorages (2017 stats for example), Average duration of anchorage: 30 hours, approximately 911 are Tankers(13%) and 5462 barges with or without tugs(80%). (Barges without tugs do not have AIS).
-Radar is the primary means of monitoring the fact that the vessels are not dragging while at anchor. If they drag anchor, we have a potential allision and marine casualty, with all sorts of negative impacts.
-Through our efforts and resources, we have avoided a Marine Casualty on the 6825 potential times it could have occurred.
- RADAR paints the vessel and gives a more accurate visual representation of the overall length. This is how VTS NY identifies the bow of the vessel and the position of the anchor when dropped. AIS transmits to location of the pilot house and would lead to less accurate swing circle plots. Swing circles are generated by the PAWSS utilizing location of the anchor, Vessel LOA, and Length of chain. VTS primarily monitors the RADAR plot while a vessel is at anchor. RADAR clearly displays changes in aspects in real time to aid in determining vessel swings, identifying potential close quarter situations and early detection of vessels dragging anchor.

2. Smaller Vessels:
-RADAR is still the primary means of tracking for a self-propelled vessel of 65 feet not engaged in commercial service, and towing vessels of 26 feet and less than 600 HP. --These vessels are VMRS Users and are not required to carry AIS. These vessels include Private Yachts, Military vessels, and 4+ towing vessels that normally operate in New York Harbor. When RADAR is not available standard routes and cameras are utilized for vessel tracking.
-Towing vessels not required to carry AIS are becoming more common in our AOR, and are difficult to track/manage
- RADAR is also the primary method for small vessel detection in NY Harbor. In the summer months smaller private vessels become more active in the Harbor. Private vessels have impeded channel restricted vessels by either becoming disabled or by fishing in or near the channels. RADAR is used in association with cameras in detecting such hazards to navigation. Additionally, RADAR is instrumental in detecting vessels that qualify for Operation Small Fry, Operation Clear Channel, and vessels encroaching Security Zones.

3. Break-aways:
a) Ships:
Over the last few years vessels breaking away from berths and moorings has become more frequent. In May 2018 a container ship parted bow lines in Port Elizabeth during severe weather. The RADAR displayed the bow of the vessel swinging off the berth almost perpendicular to the berth. The AIS location was in vicinity of the pilot house and displayed little to no movement. Detecting that the vessel was being pulled off the berth by the bow would have taken significantly more time than the real time vessel paint provided by RADAR.
b) Barges:

Additionally, Barges did not carry AIS. RADAR is a reliable sensor for barge breakaways at moorings, anchorages and berths, and depending on the location, it may be the only method for detection. Since 2018, we have more than 4 new authorized mooring areas for barges - several are in the vicinity of high traffic/congested areas. Inclement weather greatly increases the risk of these barges breaking away and causing severe damage to other vessels and/or shore facilities.

4. Debris: More sensitive radar could greatly assist us in detecting hazards to navigation. During severe weather or following severe weather, we often have 3 or 4 instances of floating debris with potential to cause damage to passing vessels - this primarily includes logs/pilings and floating docks. Due to their low sail area above the water, these are usually very difficult to detect via camera during the day, and nearly impossible to detect via camera at night.

5. ATON:
We can utilize the radar for ATON location verification. i. e. we can easily identify all the Ambrose channel marker buoys via radar. While we can't necessarily verify if the aid is on station but we can clearly see radar return on most aids - a more sensitive radar will increase/improve our ability to at least verify that the ATON is offstation.

6. AIS Failure:
Another reason we utilize the radar is for detection of vessels that are VTS users with a nonfunctioning AIS (LOD or not). We had an instance yesterday in which a vessels AIS failed shortly after getting underway. We were able to track them via radar until they exited the AOR.

*Figure 2: Radar requirements for VTS as delivered by VTS NY personnel.*

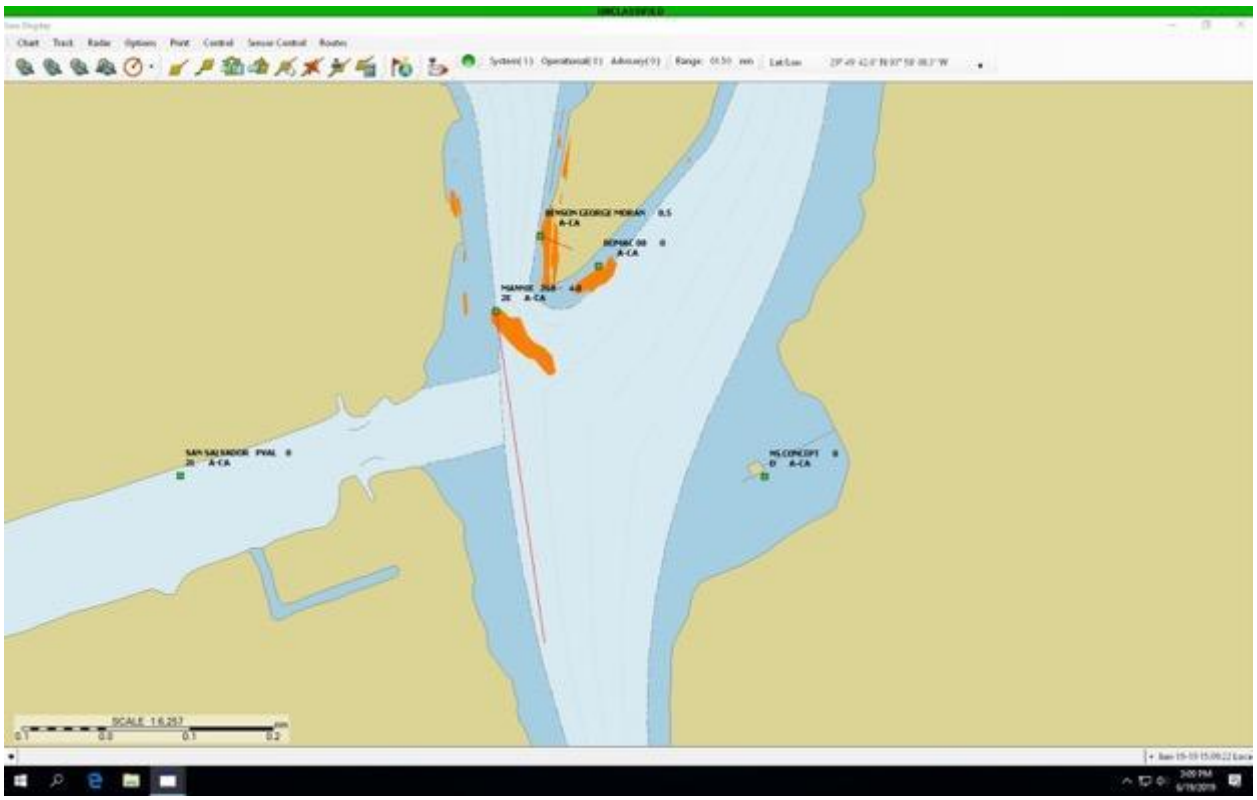


*Figure 3: Screenshot of the PAWSS situational awareness tool for VTS Port Arthur. The image shows a 45-degree difference between the AIS and radar vessel bearing.*

### 2.4.5 Project Milestones and Performance Metrics

The project milestones are listed in Table 3.

*Table 3. List of milestones defined for this research study.*

| No. | Task | Time Frame | Status |
|---|---|---|---|
| M1 | Kick-off meeting to discuss project plan, objectives, and outcomes | Months 5 | Complete |
| M2 | Release RFI | Month 8 | Complete |
| M3 | Select recommended radars | Month 12 | Complete |

The performance metrics are listed in Table 4.

*Table 4. List of performance metrics for this research study.*

| No. | Task | Time Frame | Score |
|---|---|---|---|
| PM1 | Gather requirements from at least 6 VTS centers and HQ | Months 6 | Gathered requirements from 9 VTS centers, HQ and C3Cen |

| | | | |
|---|---|---|---|
| PM2 | Submit RFI to at least 5 vendors | Month 8 | Submitted RFI to 9 radar vendors |
| PM3 | Recommend at least 2 radars for consideration | Month 12 | Complete, we recommended 8 radar vendors for consideration in next generation technology |

### 2.4.6 Transition Considerations

The Rutgers team released a request for information to radar vendors on July 31, 2020. The team utilized the responses to help inform the Coast Guard of radar vendors and models that will be sufficient for VTS usage. The team corresponded with DHS and have reviewed the responses to their RFI No. 70RSAT20RFI000004 "Unattended Sensor Technologies for Monitoring Riverine and Littoral Zone Vessel Traffic". Of the 36 respondents to that RFI, 6 of the submittals are applicable to the Coast Guard need for radar within the VTS. We plan on continuing to communicate with those 6 companies as well as others to develop radar and other sensing capabilities for the VTS mission. We also utilized the HTZ Warfare modelling software to develop a radar model for each of the VTS areas which will allow us to experiment with different radar parameters to determine if a particular radar model will fulfill the VTS mission.

The Rutgers team has met with 9 of the 12 VTS centers to compile requirements on the use of radar within the Vessel Traffic Service Centers and requirements for small vessel detection. This meets Performance Metric #1 to gather requirements from Headquarters and at least 6 of the VTS centers. Several of the VTS (New York, Puget Sound and San Francisco) stressed the need for small vessel detection to help manage the nonparticipating vessels and recreational traffic that are present within the VTS. We have located the camera and radar sensor locations within each of the VTS areas. This allows us to model the existing sensor coverage and how new radar or other sensors factor into the next generation VTS as envisioned by the Coast Guard. The Rutgers team developed a request for information (RFI) for radar and other sensor needs with respect to Coast Guard Vessel Traffic Services. We released it to 9 radar vendors which satisfies Performance Metric #2 to release it to at least 5 vendors.

The final report was delivered to the Coast Guard on June 28, 2021.

### 2.4.7 Stakeholder Engagement

The Rutgers team placed heavy emphasis on stakeholder engagement from the outset of the project. Effective stakeholder engagement focuses on building relationships with the Coast Guard based on mutual trust and understanding. Table 5 lists the Coast Guard stakeholders with whom the Rutgers team has engaged with during the project.

*Table 5. list of Coast Guard stakeholders the Rutgers team has been engaged with during the project.*

| Title | First | Last Name | Unit | Office |
|---|---|---|---|---|
| **Lt.** | Eric | Romero | 741 | Office of Shore Forces |
| **Mr.** | Brian | Page | 761 | Office of Sensor Capabilities |
| **Lt.** | Matthew | Lynne | 681 | Sustainment Program Manager for PAWSS |
| **Lt.** | Dan | Dougherty | C3-CEN | Sustainment Eng. Lead for VTS |
| **Mr.** | Darin | Mathis | CG-NAV | |
| **LCDR** | Russ | Hall | CG-771 | Requirements Officer |
| **Mr.** | Gregory | Hitchen | New York | VTS Director |
| **Mr.** | Will | Barry | New York | VTS Training Director |
| **Mr.** | Virgil | Bankes | New York | EMO |
| **Mr.** | Nick | Frascella | Louisville | VTS Director |
| **Mr.** | Johnny | O'Rourke | Houston | EMO |
| **Mr.** | Steven | Nerheim | Houston | VTS Director |
| **Mr.** | Scott | Whalen | Port Arthur | VTS Director |
| **Mr.** | John | Moore | Port Arthur | EMO |
| **Mr.** | Tony | Jones | New Orleans | EMO |
| **Mr.** | George | Petras | New Orleans | Training Officer/Coordinator |
| **Mr.** | Laird | Hail | Puget Sound | VTS Director |
| **Mr.** | Xavier | Villarreal | Puget Sound | EMO |
| **LCDR** | Thao | Nguyen | New Orleans | Director |
| **CDR** | Aurora | Fleming | Search and Rescue | Chief |
| **Mr.** | Robert | Blomerth | San Francisco | Director |
| **Mr.** | Scott | Humphrey | San Francisco | Training Officer/Coordinator |
| **ELC2** | Tom | Bound | San Francisco | EMO |
| **LT.** | Timothy | Veach | Berwick Bay | Director |
| **Mr.** | Donald | Boudreaux | Berwick Bay | EMO |
| **Mr.** | Robert | McDermott | C5i Service Center | VTS Project Manager |
| **Mr.** | Josh | Smock | C5i Service Center | PAWSS Project Manager |
| **Capt.** | Kip | Louttit | LA/LB | Executive Director, Marine Exchange |
| **Capt.** | Patrick | Baranic | LA/LB | Ops. and Training Manager, Marine Exchange |
| **OSC.** | Casey | Robert | LA/LB | VTS Director |

### 2.4.8 Potential Programmatic Risks

The project has been successfully completed. The final project report and appendices have been submitted to DHS.

### 2.4.9 Progress Against Milestone Outcomes

All milestones were successfully completed on time.

### 2.4.10 Unanticipated Problems

The COVID-19 pandemic prevented the research team from completing all the in-person visits to the Vessel Traffic Service (VTS) centers as originally outlined in the work plan. With the help of Lt. Eric Romero, USCG Office of Shore Forces, we were able to conduct phone interviews with the remaining VTS centers to gather requirements for radar and other sensors within the VTS operations.

### 2.4.11 Information Supported by Data

**VTS Activity Reports**

Mr. Darin Mathis, CG-NAV, provided monthly transit data for each of the VTS centers which are all vessels that are considered “active tracks”. The transit data is comprised of ferry passenger, freight, tankers, tug/tow and other. A summary plot of the data is provided in Figure 5. The VTS centers break into 3 categories as shown in Table 6 greater than 10,000 monthly transits, between 10,000 and 1,000, and less than 1,000 monthly transits. This provided the team with a scale for the volume of traffic that each VTS needs to manage.

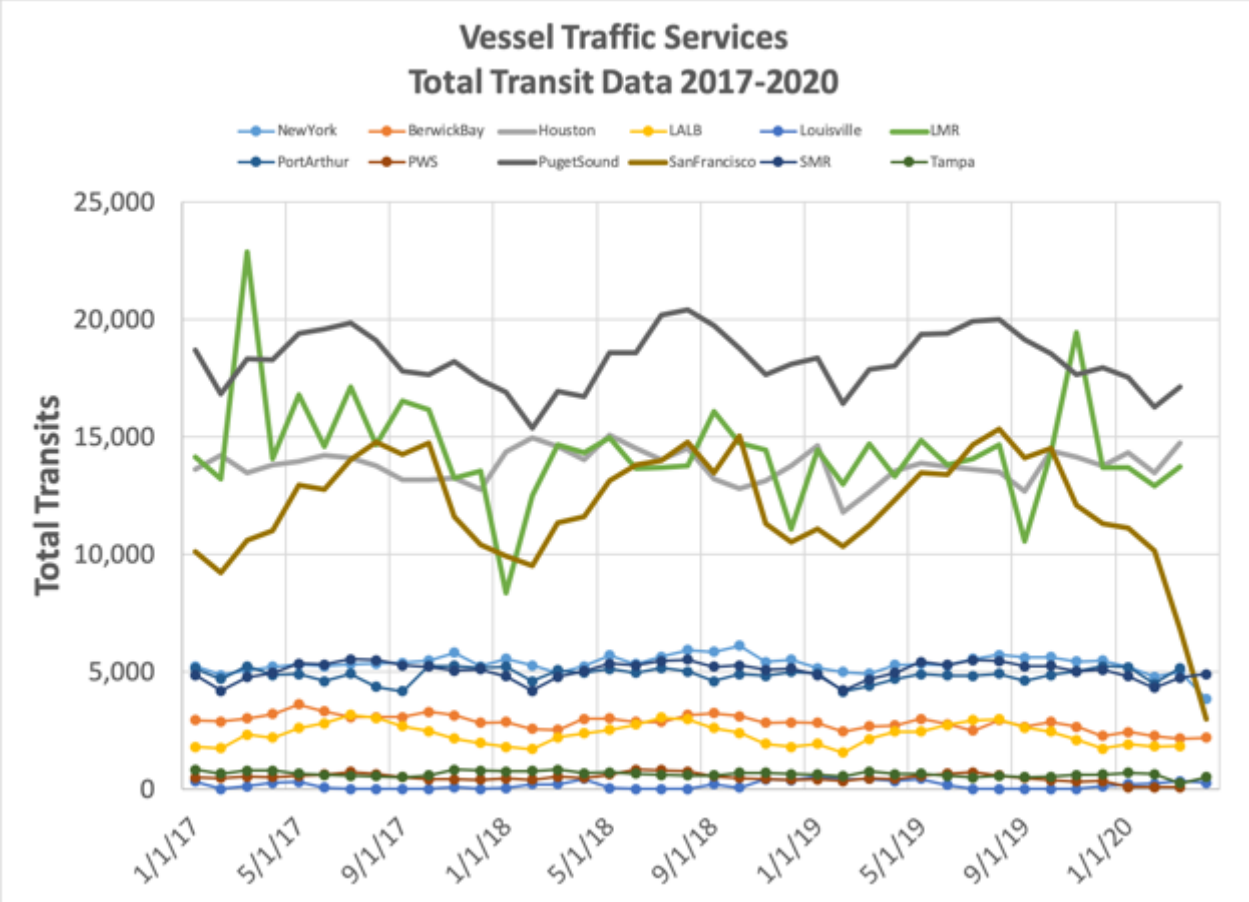



Figure 5. Three-year *(January 2017 to April 2020) record of VTS transit data. The legend for the particular VTS location is provided at the top of the figure.*

*Table 6: Breakdown of VTS centers by monthly transit activity.*

| Greater than 10,000 | Greater than 1,000 | Less than 1,000 |
|---|---|---|
| Puget Sound | New York | Louisville |
| San Francisco | Port Arthur | Prince William Sound |
| Lower Mississippi River | Berwick Bay | Tampa |
| Houston/Galveston | Los Angeles-Long Beach | |
| | St. Mary's River | |

**Geospatial Analysis**

The MSC research team discovered that the area of responsibility (AOR) for each VTS had been developed into a GIS shapefile as part of a National Transportation Safety Board study [4]. Dr. Eric Emery, Chief, Safety Research Division NTSB was able to deliver the shapefile to the team. This saved the project of having to recreate the data file. An example of the shapefile is provided in Figure 6 which shows the AOR for VTS New York. Having the shape

file allowed the team to calculate the area that each VTS is responsible for as shown in Figure 7. The figure displays the VTS locations ranked from smallest AOR (Louisville 6 $mi^2$) up to the largest (Puget Sound 2,980 $mi^2$).

*Figure 6. GIS shapefile visualization for VTS New York shown as the yellow area.*

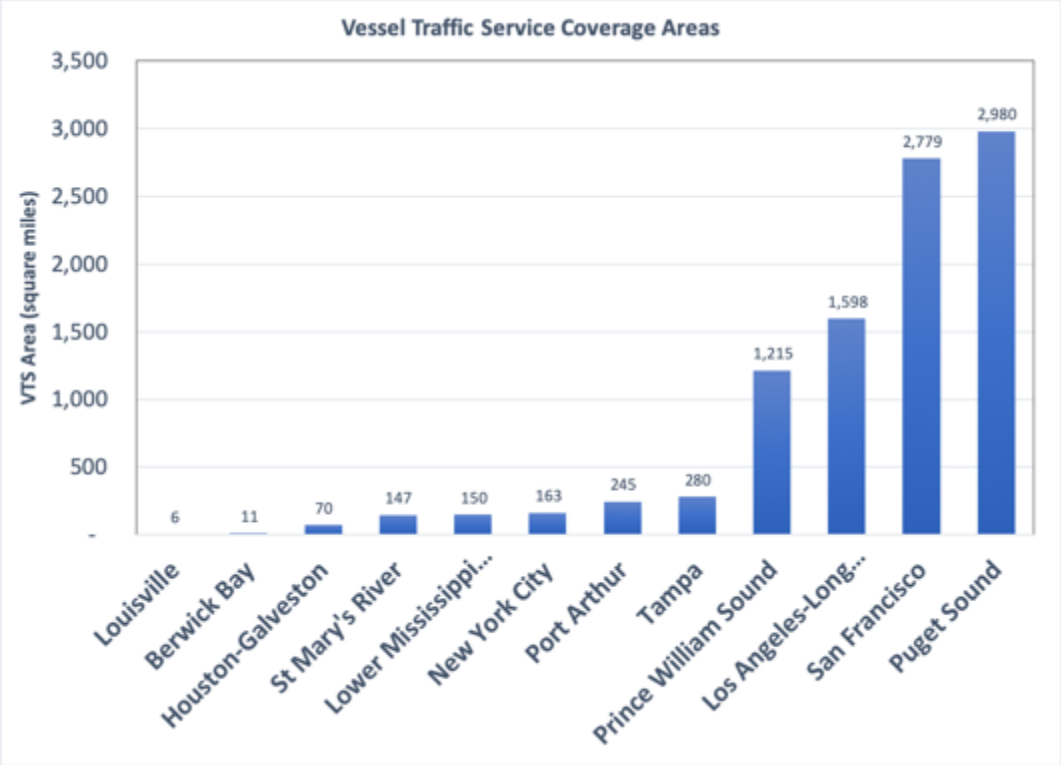



*Figure 7. Area of responsibility (square miles) for each of the VTS locations.*

**VTS Remote Locations**

We have complied the most up to date locations of radar and camera locations within each of the VTS centers. The Rutgers team has used the information on the sensor type and location to develop models of each VTS to determine how well the VTS area is covered by sensors. Figure 8 provides a map of VTS NY showing regions where there is only 1 sensor coverage (tan) and greater than 1 sensor coverage (rusty red). This map shows there is only a small portion of the VTS not covered by sensors (western side of Raritan Bay) and also indicates that the majority of the VTS has redundant coverage which is a positive note for the resiliency of the VTS to outages. Another type of analysis the team will conducted in the second half of the project is HTZ modelling of radar coverage. An example of this type of analysis is shown in Figure 8. This allowed the team to experiment with radar particulars (power, frequency, bandwidth, model type) to determine the efficacy of the radar choice for the next generation VTS.

Table 7 provides a status of geospatial analysis for radar and camera coverage within each of the VTS areas. Green indicates analysis that is complete, yellow shows analysis that is underway and red for analysis that is planned.

*Table 7: Status of geospatial analysis of each of the VTS areas. The legend is located at the top of the table*

| **Geospatial Analysis Progress by Program**<br>Status: ● Planned ● Underway ● Completed | | | | |
|---|---|---|---|---|
| **VTS No.** | **Vessel Traffic Service** | **Google Earth** | **ArcGIS PRO** | **HTZ Warfare** |
| 1 | New York | ● | ● | ● |
| 2 | St. Mary's River | ● | ● | ● |
| 3 | Louisville | ● | ● | ● |
| 4 | Tampa | ● | ● | ● |
| 5 | Lower Mississippi River | ● | ● | ● |
| 6 | Berwick Bay | ● | ● | ● |
| 7 | Port Arthur | ● | ● | ● |
| 8 | Houston/ Galveston | ● | ● | ● |
| 9 | Los Angeles/ Long Beach | ● | ● | ● |
| 10 | San Francisco | ● | ● | ● |
| 11 | Puget Sound | ● | ● | ● |
| 12 | Prince William Sound | ● | ● | ● |

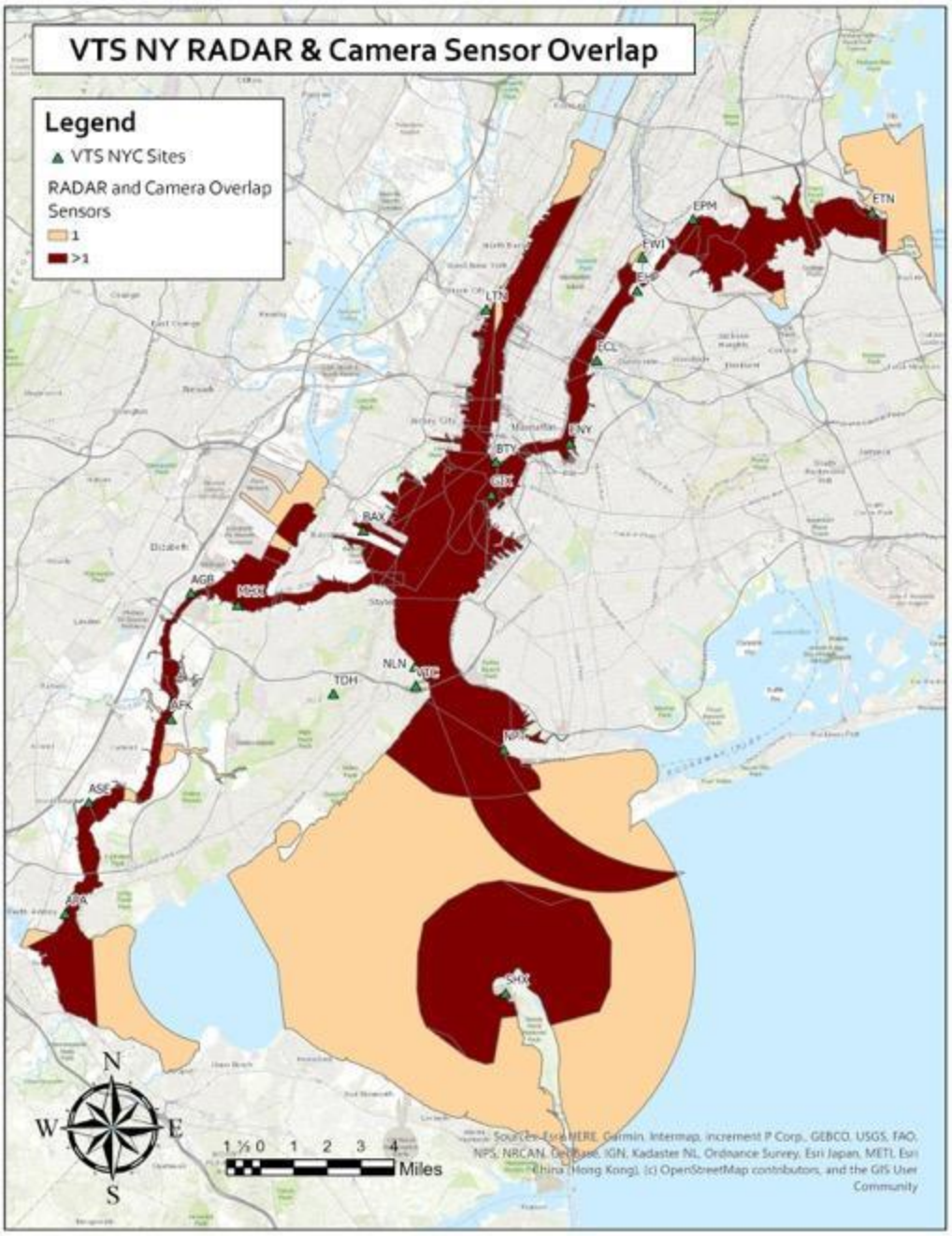



*Figure 8. Map showing the radar and camera coverage of VTS NY. The colors indicate areas where there is only one sensor type covering the VTS (tan) and greater than one sensor type (rusty red).*

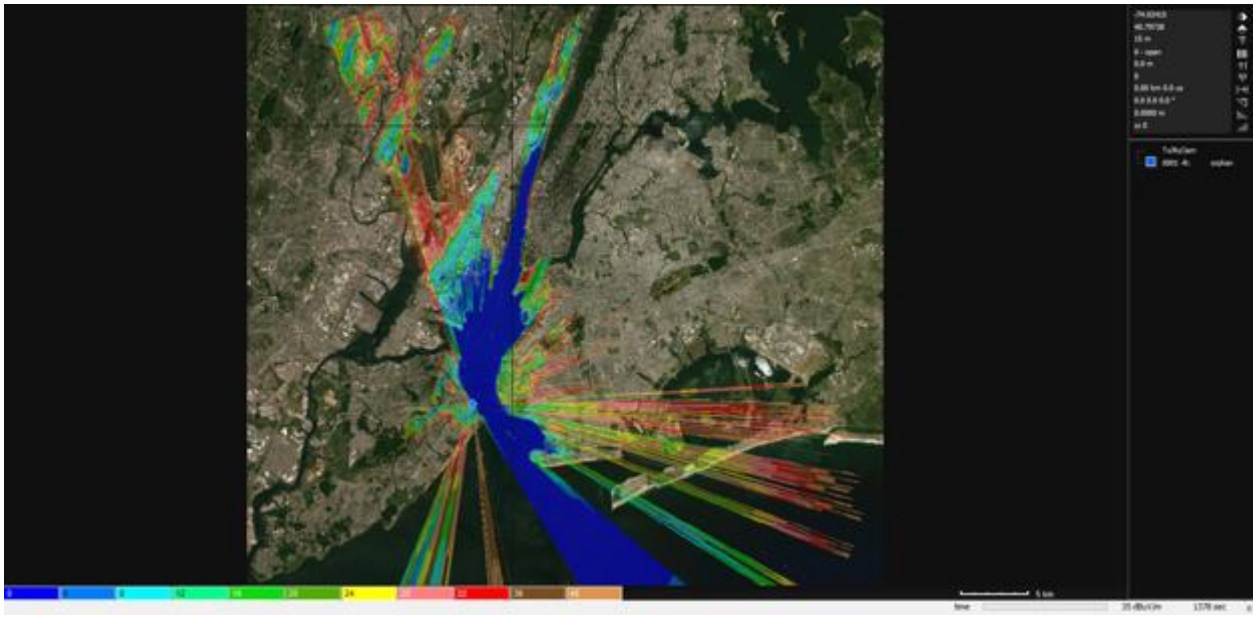


*Figure 9. HTZ modelling of radar coverage for the New Lane radar site within VTS NY. The colors indicate the height of the target that radar is capable of detecting (blue - smallest up to brown - largest).*

**Request for Information**

We released the Request for Information on July 31, 2020. The RFI was modelled after DHS RFI 70RSAT20RFI000004 “Unattended Sensor Technologies for Monitoring Riverine and Littoral Zone Vessel Traffic”. A copy of the RFI can be found in the final project report submitted to DHS in June 2021.

The list of respondents for next generation VTS are presented in Table 8.

*Table 8: List of companies that responded to RFI grouped by technology type.*

| | | | | |
|---|---|---|---|---|
| Radar | ELTA NORTH AMERICA | FLIR | FURUNO | GEM elettronica |
| | HENSOLDT Detect and Protect. | navico | Sperry Marine | TERMA |
| Camera | FLIR | ISA Innovative Signal Analysis, Inc. | PHAROVISION | |
| Hardware | SSR | | | |
| Software | NOBELTEC | | | |

After the MSC research team developed a radar use questionnaire that was utilized in a series of interviews with VTS centers to assess existing and future remote sensing needs for VTS operations, the team drafted the RFI that was distributed to radar and sensor vendors. The team also analyzed previous studies by Lockheed Martin of VTS areas as well as current studies by Canadian Coast Guard for their Vessel Traffic Services which helped contribute to the RFI. The received responses were tabulated to determine which radar features would provide the greatest benefit for the VTS mission.

In addition to the RFI work, MSC researchers analyzed Automatic Identification System (AIS) and VTS transit data to develop a picture of the traffic within each VTS. The team also performed a geographic analysis of existing radar and camera coverage within each VTS to determine sensing resiliency and identify any potential gaps in the sensor network. The RFI, RFI response analyses, and other technical data are available in the project's final report.

**References**


[1]. "U.S. Port Ranking By Cargo Volume". American Association of Port Authorities. 2013. Retrieved October 9, 2015.

[2] "Capability Analysis Report for Vessel Traffic Service". United States Coast Guard. August 22, 2019, Version 01

[3] "Vessel Traffic Service Radar Research Project" Final Report, Stevens Institute of Technology, Maritime Security Center, November 30, 2017

[4] National Transportation Safety Board. 2016. An Assessment of the Effectiveness of the US Coast Guard Vessel Traffic Service System. Publication Type NTSB/SS-16/01. Washington, DC.


# 3 Education and Outreach

MSC is committed to enhancing the knowledge, technical skills and leadership capabilities of the Nation's current and prospective maritime security workforce. At the core of the Center's mission is the transfer of its research and expertise into relevant, innovative educational programs for undergraduate and graduate STEM students, and professional development opportunities for homeland security professionals and Minority Serving Institution (MSI) faculty. The Center's portfolio of educational programs for Year 7 includes:

- The Summer Research Institute (SRI)
- Research Assistantship Program
- Minority Serving Institution (MSI) Engagement Workshop
- MSI Summer Research Team Program
- Maritime Cybersecurity Professional Development Course

## 3.1 Summary of Education Milestones

### 3.1.1 Summer Research Institute (SRI)

MSC held its 12th annual Summer Research Institute, virtually during Year 7. The 2021 SRI program included 14 students representing four U.S. universities, including two Minority Serving Institutions. The students were organized into five research teams. MSC's stakeholders provided input into student research project topics and served as webinar speakers, subject matter experts and project mentors throughout the program. Video recordings of the student research presentations as well as copies of their power point slides and research posters can be found on the SRI program webpage at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021.

### 3.1.2 Undergraduate and Graduate-level Research Assistantships

MSC provided tuition and stipend support for two Graduate Research Assistants during the 2020/2021 academic year. As part of their Assistantship requirements, the students engaged in 20 hours per week of research and contributed to projects initiated in the MSC's Summer Research Institute 2020 program.

In addition to the two graduate students, MSC engaged four undergraduate students in research tasks and projects throughout the academic year. Funding support for the undergraduate students was provided by Stevens Institute of Technology.

### 3.1.3 MSI STEM Educator's Workshop

The MSC held a workshop for Minority Serving Institution (MSI) STEM educators on April 30, 2021. The topic of the workshop was *Cybersecurity in the Maritime Transportation System and other Critical Infrastructure*. The objective of the annual workshop series is to share subject matter expertise and provide professional development opportunities and resources for educators working within underrepresented and underserved communities. Attendees included representatives from four MSI schools, together with stakeholders from the USCG and DHS S&T.

### 3.1.4 MSI Summer Research Team Program

MSC hosted faculty and student research teams from Norfolk State University (NSU) and North Carolina Central University (NCCU) as part of the DHS MSI Summer Research Team (MSI SRT) program. The NSU and NCCU teams participated in the Center's virtual Summer Research Institute and conducted research in the areas of cybersecurity risks in offshore wind farms, and GIS and data visualization of USCG MISLE data. The team's presentation slides, and a recording of their final research presentation can be found on the MSC Summer Research Institute webpage. (https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021)

### 3.1.5 Maritime Cybersecurity Professional Development Pilot Course

MSC in conjunction with Coast Guard Cyber Command and USCG Sector New York developed a Maritime Cybersecurity pilot course tailored to Coast Guard marine safety

personnel. The professional development course was originally planned to be held in April 2020, however, due to the COVID pandemic the pilot course was postponed and held virtually on October 1 and 2, 2021 for a cohort of 13 USCG participants from LANTAREA, and again on December 3 and 4, 2021 for a cohort of 19 USCG personnel from PACAREA. Participants in the course received a certificate of participation, 1.3 continuing education units and a post program student survey was conducted.

## 3.2 The Summer Research Institute (SRI)

### 3.2.1 Milestones and Performance Metrics

| # | **Milestone** | **Performance Metric** | **Output** |
|---|---|---|---|
| M1 | Featured lectures by MSC researchers and guests. (5/17/21 – 6/25/21)* | A minimum of two homeland security/maritime industry guest speakers will be hosted during the 2021 summer research program. | Completed: The MSC hosted four guest webinars and engaged more than 17 homeland security professionals in conversations with the student research teams. |
| M2 | Field-visits and field-based activities. (5/17/21 – 6/15/21)* | Students will engage in a minimum of one field-based activities during the summer research program.<br><br>If the COVID pandemic prohibits field-based visits and activities during the 2021 program, the MSC will feature a minimum of two DHS guest speaker webinars. (USCG and CBP) | Completed: Four guest webinars were held during the SRI 2021 program, including representatives from the USCG and DHS S&T. Due to the COVID pandemic, no group field-visits occurred. |
| M3 | Diversity of student participants (5/17/21 – 6/25/21)* | Diversity will be measured according to the number of students from underrepresented communities (MSI schools, minority students and women), and to the number of STEM disciplines represented in the program. A minimum of four different | Completed: 71% of the student participants were from underrepresented communities (women and minority students). The SRI cohort included students |

| | | | |
|---|---|---|---|
| | | disciplines will be represented. | from 9 academic disciplines. |
| M4 | Research reports, presentations, and posters (6/21/21 – 6/25/21)* | A minimum of one research summary report and research poster will be prepared at the culmination of the SRI 2021 program. | Completed. Five student reports, presentations and posters were prepared. |
| M5 | Post-program student survey. (6/21/21 – 6/25/21)* | A minimum of one student survey will be conducted at the end of the 2021program. The survey will be used to measure student learning gains and program impacts on research and career interests. | Completed: A student survey was conducted to assess the impact of the SRI program. 11 out of the 14 student participants completed the survey. |

*The Center's education program Year 7 work plan called for the program to be held over a six-week period, however, in order to leverage external funding to support DHS MSI Summer Research Team and Stevens Pinnacle and Clark Scholars, MSC accommodated students and faculty with 10-week program requirements.

### 3.2.2 Overview

MSC offers an annual STEM-focused summer research program designed to expose undergraduate and graduate-level students to the maritime and homeland security domain. The goal of the Summer Research Institute (SRI) is to connect students with homeland security researchers and practitioners, and to engage them in research projects that are responsive to the knowledge and technology needs of the homeland security enterprise. Due to the ongoing COVID pandemic the Center's 12$^{th}$ annual Summer Research Institute was held online, for a second year in a row. The Center's Year 7 workplan called for the program to be held over a six-week period, however, in order to leverage external funding to assist in supporting student engagement, MSC accommodated students with 10-week program obligations, including Stevens Pinnacle Scholars, Stevens Clark Scholars and faculty and student participants in the DHS MSI Summer Research Team program.

The summer research program included 14 students. Altogether they represented four universities, including Columbia University, Norfolk State University (MSI school), North Carolina Central University (MSI school) and Stevens Institute of Technology. 13 out of the 14 student participants were undergraduates, and 71% were from underrepresented communities (e.g., women and minority students)

To offset the costs of the SRI (e.g., faculty costs, etc.), the Center leveraged existing Stevens Institute of Technology programs to recruit students who could attend the program fully funded through external funding sources. Out of the 14 program participants, six students attended the program leveraging funding from Stevens Institute of Technology,

including the university's Pinnacle Scholars Program (3), and Clark Scholars Program (3), and three students attended the program through the DHS Minority Serving Institute Summer Research Team Program (MSI SRTP). Funding for the remaining five students was provided by the Maritime Security Center.

The MSC-funded students were selected through the Center's academic partnerships and through a competitive admission process. The students admitted into the program were endorsed by their academic professors and met or exceeded the Center's admission criteria. Figure 1 shows the collective images of the SRI 2021 student research teams and Table 1 identifies the participants and the funding sources leveraged to support their participation.

The SRI 2021 student projects were determined several months prior to the start of the program, and were developed in conjunction with the Center's colleagues at USCG Sector NY. Collectively, the student participants were organized into five research project teams. Discussions on each of these projects follows below in section 3.2.8.


*Figure 1. The SRI 2021 program was held virtually due to the ongoing COVID pandemic. Weekly group sessions and student team meetings were held via Zoom.*

*Table 1. Summer Research Institute Student Participants and Leveraged Funding.*

| **University** | **Student** | **Major** | **Funding Source** |
|---|---|---|---|
| Columbia University | Dairon Estevez | Mechanical Engineering | MSC |
| Norfolk State University | Tricia Camaya<br><br>Zaid Abdul-Kaudeyr | Information Security & Assurance<br>Computer Science | DHS MSI Summer Research Team Program (MSI SRT) |

| | | | |
|---|---|---|---|
| North Carolina Central University | Isabel Gutierrez | Geographic Information Systems | DHS MSI Summer Research Team Program |
| Stevens Institute of Technology | Ron Dumalagan<br>Reva Grover<br>Erin Harrison<br>Xinyuan Luo<br>Victor Mavricos<br>Tara McLoughlin<br>Andrew Narvaez<br>Kristina Sunada<br>Mehrab Syed<br>Samantha Weckesser | Computer Science<br>Systems Engineering<br>Civil Engineering<br>Applied Mathematics<br>Civil Engineering<br>Cybersecurity<br>Computer Science<br>Mechanical Engineering<br>Software Engineering<br>Software Engineering | Clark Scholar<br>MSC<br>Pinnacle Scholar<br>Pinnacle Scholar<br>MSC<br>Clark Scholar<br>MSC<br>Pinnacle Scholar<br>MSC<br>Clark Scholar |

### 3.2.3 Student Qualifications and Documentation

Participation in the SRI requires that students be actively enrolled in an undergraduate or graduate-level degree program at an accredited university. Undergraduate students must possess a minimum GPA of 3.0, and graduate-level (Masters and PhD) students are required to have a GPA of 3.5 or better. As part of the application process, student participants were required to complete an online application form, write a personal statement of interest, submit letters of recommendation and transcripts upon request.

### 3.2.4 Summer Research Stipends

MSC-funded students received a summer stipend of $4,000 dispersed in two equal payments of $2,000 at the start and end of the program.

### 3.2.5 Program Administration

The 12th annual SRI was organized and coordinated by MSC Director of Education, Beth Austin-DeFares in conjunction with Dr. Barry Bunin (Research Professor, Civil, Environmental and Ocean Engineering). Ms. Austin-DeFares served as the primary program facilitator, while Dr. Bunin participated as a faculty mentor and curriculum developer. He also served as the overall technical lead on the summer research projects and provided assistance to students in both theoretical and practical implementation of their projects. SRI student team mentorship was also provided by Dr. Brendan Englot, Director of the Robust Field Autonomy Laboratory and Assistant Professor in Mechanical Engineering at Stevens Institute of Technology, Dr. Mary Ann Hoppa, Associate Professor, Norfolk State University (NSU), Dr. Rakesh Malhotra, Associate Professor, Environmental, Earth and Geospatial Sciences, North Carolina Central University (NCCU) and Dr. Hugh Roarty, Research Project Manager, Rutgers University.

### 3.2.6 Program Format and Curriculum

The virtual program included faculty lectures, a series of homeland security webinar speakers, and stakeholder-focused research projects. Prior to the start of the program, the students were organized into one of the following five project teams and were provided with information on their respective team assignments:

- BlueROV – Advancing the capabilities of an underwater remotely operated vehicle.
- Understanding Cybersecurity Risk in Offshore Wind Farms
- Improved USCG HAZMAT Cargo Inspections
- Geographic Information Systems and Coast Guard data visualization
- Cybersecurity and Data Analysis – USCG Sector New York field-based internship project

During Week One of the program the students were given reading and homework assignments. The students then attended introductory lectures via Zoom, delivered by Dr. Barry Bunin. The lectures oriented the student group to the maritime and homeland security domain, and included topics related to maritime security policies, current and emerging threats in the maritime domain, and an overview of port facility infrastructure and operations.

Starting Week Two, the students began to meet a minimum of three times per week with their faculty mentors and teammates and attended guest webinars provided by MSC's DHS colleagues and stakeholders.

During Weeks Three - Seven, the student teams began to provide status reports on their research projects in the form of weekly status update presentations. Each team was responsible for providing a ten-to-fifteen-minute slide presentation discussing their research topic, the team's progress and research activities, and any challenges they were encountering. Throughout this time period, MSC administrators also arranged for the student teams to meet virtually one-on-one with subject matter experts in the fields of maritime safety and security, port security, offshore wind farms, and cybersecurity and critical infrastructure protection. Some of the student teams were also invited to provide research briefings to USCG Sector NY, USCG Sector VA, Customs and Border Protection Field Operations, and Idaho National Laboratory personnel.

During Weeks Six - Ten, the student teams synthesized their research outcomes and started to prepare their final reports, presentations and research posters. In Week Eight, the students presented their research in a virtual presentation event for the Center's DHS stakeholders. More than 23 DHS and homeland security personnel attended the virtual presentation event, including representatives from the DHS S&T network (NUSTL and the Office of University Programs), CBP, USCG (USCG HQ and Sectors New York), as well as other Federal and state organizations including the Bureau of Ocean Energy Management (BOEM), Center for Prevention Programs and Partnerships (CP3), Port Authority of New York and New Jersey, and the Texas Military Department, among other representatives from industry and academia.

Tables 2 and 3 below illustrate the program activities and webinar speakers for each week of the 2021 summer research program.

*Table 2. SRI 2021 Program Activities.*

| Schedule | Topic | Faculty /Guest Speakers | SRI 2021 Activities |
|---|---|---|---|
| Week One<br>May 17 - 21 | MTS and Maritime Security Overview | Faculty: Dr. Barry Bunin | Reading and homework assignments. Group orientation and discussions/lectures on maritime security and vulnerabilities. |
| Week Two<br>May 24 - 28 | Team Research Projects | Webinar Speakers:<br>John Hillin, Safety and Security Division Chief, Sector NY | Webinar presentations and SRI group and student research team meetings via Zoom. HAZMAT Cargo team meets with J. Hillin and I. Lennard, National Cargo Bureau |
| Week Three<br>May 31 – June 4 | Team Research Projects | Webinar Speakers:<br>Bert Macesker, Executive Director and Lew Lewandowski, Chief, Environment and Waterways Branch, USCG RDC | Webinar presentations and SRI group and student research team meetings via Zoom, including student team weekly status update presentations. |
| Week Four<br>June 7 – 11 | Team Research Projects | Webinar Speakers:<br>Stephanie Okimoto, Director, International Cooperative Programs Office, and Mr. Kevin K. Adams, Marine Transportation System (MTS) Cybersecurity Specialist, USCG First District<br><br>Guest attendee for the student status update presentations: Greg Simmons, DHS OUP | Webinar presentations and SRI group and student research team meetings via Zoom, including student team weekly status update presentations.<br><br>Cyber Wind farm team briefs Dr. Gary Kessler, author Maritime Cybersecurity: A Guide for Leaders and Managers. |
| Week Five<br>June 14 – June 18 | Team Research Projects | Guest attendee for the student status update presentations: Dr. Beth White, ORISE | Student research team and SRI group meetings, including student team weekly status update presentations. |

| | | | |
|---|---|---|---|
| | | | BlueROV team briefs USCG Sector NY representatives. |
| Week Six June 21 – 25* | Team Research Projects | | Student team weekly status update presentations. |
| Week Seven - Ten June 28 – July 23* | Research Synthesis<br><br>Virtual Student Research Presentations | Hazmat Cargo team briefing with Sector VA<br><br>DHS S&T stakeholders & industry guests (USCG, CBP, DHS S&T, NUSTL, BOEM) attended the students final presentation session on July 8. | Report writing, presentation slide preparation and research posters. Status update presentations and rehearsals.<br><br>HAZMAT Cargo Team briefs USCG Sector VA representatives.<br><br>SRI student research teams presented their research in a virtual presentation event held via Zoom on July 8, 2010.<br><br>Completion of SRI project deliverables. (e.g., presentation recordings, posters, final reports and research poster.)<br><br>Completion of SRI feedback survey. |

*The Center's education program Year 7 work plan called for the program to be held over a six-week period, however, in order to leverage external funding to support DHS MSI Summer Research Team and Stevens Pinnacle and Clark Scholars, MSC accommodated students and faculty with 10-week program requirements.

*Table 3. SRI 2021 Webinar Speakers and Subject Matter Experts Engaged.*

| **Guest Speaker** | **Organization** | **Lecture / Engagement** |
|---|---|---|
| Mr. Kevin Adams, Marine Transportation System Cybersecurity Specialist | USCG First District | Webinar: MTS Cybersecurity Program Overview: Support Capabilities & Case Studies |
| MST1 Christian Applegate | USCG Sector NY | Meetings and mentorship of the HAZMAT Cargo team. |

| | | |
|---|---|---|
| MSTC Ryan Chartier, and MST2 Alex Evans | USCG Sector VA | Meeting with the HAZMAT Cargo team |
| Mr. Jake Gentle, Senior Power Systems Engineer | Idaho National Laboratory | Meeting with the Cyber Wind farm team |
| BOSN3 Jason Grimm, USCG Sector NY and BM1 Eric Brosnihan**,** | USCG Sector NY | Meeting with the BlueROV team |
| Mr. John Hillin, Safety and Security Division Chief | USCG Sector NY | Webinar: *Cargo Containers and Hazardous Materials*, and meetings and mentorship of the Hazmat Cargo and GIS teams |
| Dr. Gary Kessler, Author and Dr. David Burke (Fathom5) | *Maritime Cybersecurity: A Guide for Leaders and Managers* and Fathom5 | Meeting with the Cyber Wind farm team. |
| Mr. Ian Lennard, President | National Cargo Bureau | Meetings with the Hazmat Cargo team. |
| Mr. Bert Macesker, Executive Director and Mr. Lew Lewandowski, Chief, Environment and Waterways Branch | USCG Research and Development Center | Webinar: Coast Guard UxS Discussion *-from Big Picture Strategy to Port Subsurface Capabilities Development* and suggested CG mission use cases for the BlueROV project. |
| Mr. Noel Moloney, Supervisor, Seaport Antiterrorism Team | CBP Field Operations Port of NY/Newark | Meeting with the BlueROV team |
| Stephanie Okimoto, Director, International Cooperative Programs Office | DHS S&T | Webinar: DHS International Programs and Partnerships Briefing |
| Mr. Scott Rutledge, Watch Commander and Mr. Michael Vernon**,** Supervisory CBPO | CBP Field Operations Port of NY/Newark | Meeting with the Hazmat Cargo Team |

### 3.2.7 Meetings with Homeland Security Professionals

Due to the ongoing COVID-19 pandemic, the MSC held its 12th annual summer research program virtually. In lieu of the program's annual field visits to ports and homeland security facilities, the Center organized a series of webinar speakers and created

opportunities for the student teams to meet with a broad range of homeland security professionals via Zoom, WebEx and Microsoft Teams.

Interactions with professionals in the maritime and homeland security domain are a key feature of the Center's summer research program. It is through these meetings and interactions that students are able to learn first-hand about the current state of affairs in the field and to better understand stakeholder and end-user needs. Student/stakeholder interactions also provide an opportunity for MSC's stakeholders to observe and engage with student talent and to contribute to the education of homeland security career-focused students. These engagements also provide students with the opportunity to learn about jobs and careers that they may not have known about otherwise.

### 3.2.8 Student Research Projects

The topics for the SRI 2021 student research projects were developed in conjunction with the Center's stakeholders, in particular the USCG Sector New York. The summer research projects and student team assignments are described in detail below.

**Research Team/Project: *Cybersecurity Risks of Offshore Wind Farms***

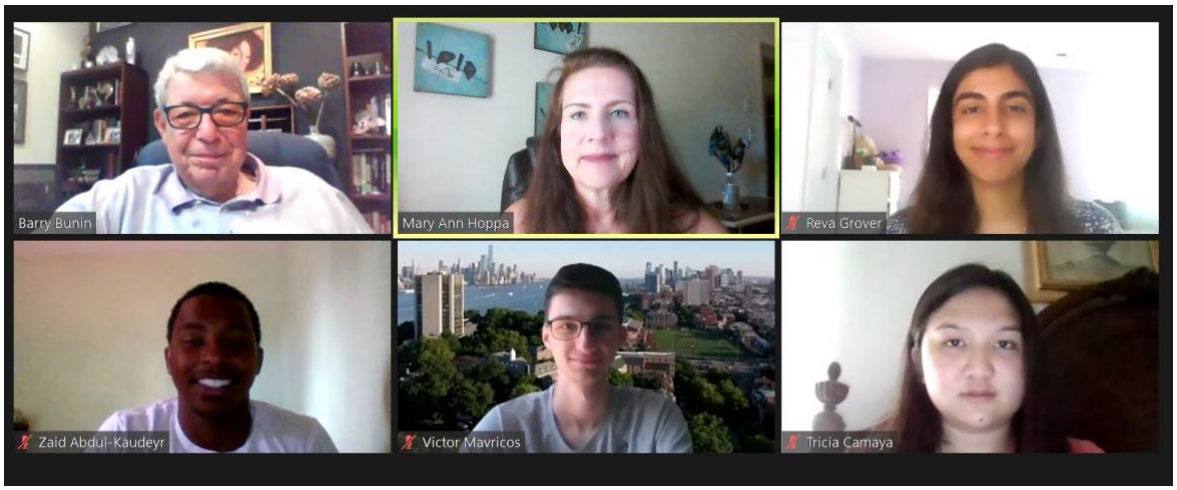



*Figure 2. Students on the Cybersecurity Risks of Offshore Wind Farm team assessed potential cybersecurity risks and vulnerabilities in offshore wind farm installations.*

The Cybersecurity Offshore Wind Farm team was tasked with understanding the potential cybersecurity threats and vulnerabilities associated with offshore wind farms and the prospective risks that they may pose to critical infrastructure and maritime operations. With increasing interests and investments in renewable energy sources, offshore wind farms are quickly emerging in US coastal waters with the goal of providing power to more than 10M homes by 2030. While much analysis to date have largely focused on environmental impacts, health concerns and efficiency and capacity, little focus has been placed on the cybersecurity risks of wind farms and their connectivity to the power grid, or the prospective impacts to maritime operations should an offshore wind turbine or network of turbines be compromised or incapacitated.

During their summer research program, the team had the opportunity to meet with and discuss their research with Dr. Gary Kessler, author *Maritime Cybersecurity: A Guide for Leaders and Managers,* and with research scientists from Idaho National Laboratories. Outcomes from the team's research resulted in the development of an Offshore Wind Farm Learning Tool developed to provide resource and learning materials, as well as information on potential cybersecurity concerns and vulnerabilities. The Offshore Wind Farm Learning Tool can be found on GitHub at: https://owflearning.cyberwaze.org/

At the end of the summer research program, Dr. Mary Ann Hoppa, the lead faculty mentor for the team, was extended an invitation to discuss the team's research at the 2021 Hack the Sea DEFCON event held virtually August 5-8, 2021. (https://hackthesea.org/)
Dr. Hoppa and her student research team from Norfolk State University (NSU), participated in the MSC's Summer Research Institute through funding by the DHS Minority Serving Institution Summer Research Team (MSI SRT) program. The team plans to apply for available follow-on funding through the MSI SRT program to continue their research. An overview of the student team's research including the team's research question, methodology and outcomes are provided below in Table 4.

*Table 4. SRI 2021– Cybersecurity Risks in Offshore Wind Farms Project Overview.*

| **Project Title: Cybersecurity Risks of Offshore Wind Farms** |
|---|
| **Research Question:**<br>● *To determine the extent to which offshore wind farms may pose a genuine cybersecurity threat to maritime operations and critical infrastructure.* |
| **Importance to Homeland Security:** The United States is becoming increasingly dependent on wind energy. The Biden administration plans to implement 30 megawatts of offshore wind power that would supply 20 percent of electricity needs by 2030. Protecting offshore wind farms from cybersecurity threats is crucial to protecting the Nation's energy critical Infrastructure. |
| **Prospective End-users:** U.S. Coast Guard, BOEM and general audiences |
| **Abstract:** With the current emphasis on renewable energy resources, wind power is on everyone's mind including United States (US) President Joe Biden, who plans to implement 30 gigawatts of offshore wind turbine energy by the year 2030, enough to power over 10 million American homes. Highly digitized and interconnected modern wind farms, both onshore and offshore, must be considered as potential sources of cyber risk to US critical infrastructures (CI) such as the power grid and maritime operations. Due to the newness of offshore wind farms (OWF), much about their specific cybersecurity vulnerabilities remains unexplored. Limited sharing of open-source information makes it difficult to understand their complex information and operational technologies (IT/OT) and possible attack vectors. Furthermore, new cyber threats and vulnerabilities involving people, processes, and technologies are constantly emerging. Despite mitigations, attackers continue to find new ways to break through cyber defenses. This project analyzed the extent to which OWFs may play a role in cybersecurity threats to maritime operations and CI by considering the IT/OT elements in a typical OWF, and their nodal connections. Rationales are |

| |
|---|
| presented for why OWFs are susceptible to various cyber-attacks. A significant likely scenario involves leveraging the onshore control center to gain access to the communications network to inject malware that is transmitted to the wind turbines to disable or catastrophically damage them. Walking through such scenarios and explaining their immediate and widespread impacts on CI and maritime operations leads to a call to action for securing the country's renewable energy sooner rather than later in light of today's cyber-dominated environment. The creation of an online learning tool is described that was used to capture the knowledge developed during this analysis including potential vulnerabilities, potential attack scenarios, frequently asked questions, and a curated library of key resources to jump-start those who need to quickly understand and make decisions related to OWFs. |
| **Methodology:** The team performed a literature review and consulted with subject matter experts throughout the SRI program. The team learned to code to develop an html-based educational tool. |
| **Research Outcomes:** The student team developed plausible scenarios in which offshore windfarms could be hacked and compromised. The team developed an Offshore Wind Farm Learning Tool that illustrates the components of an offshore wind farm and how they are vulnerable to cyber-attacks. (https://owflearning.cyberwaze.org/) |

A copy of the Offshore Wind Farm team's final research presentation slides, including a recording of their presentation and research poster can be found on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021.

Table 5 below identifies the team, their academic majors and university affiliations.

*Table 5. Cybersecurity Risks in Offshore Wind Farms Team Members.*

| **Student** | **Academic Discipline** | **School** |
|---|---|---|
| Zaid Abdul-Kaudeyr | Computer Science | Norfolk State University |
| Tricia Camaya | Information Security & Assurance | Norfolk State University |
| Reva Grover | Systems Engineering | Stevens Institute of Technology |
| Victor Mavricos | Civil Engineering | Stevens Institute of Technology |
| **Faculty Mentors:** Dr. Mary Ann Hoppa, Norfolk State University and Dr. Barry Bunin, Stevens Institute of Technology | | |

**Research Team/Project: *Risk Management and Analytics Dashboard***

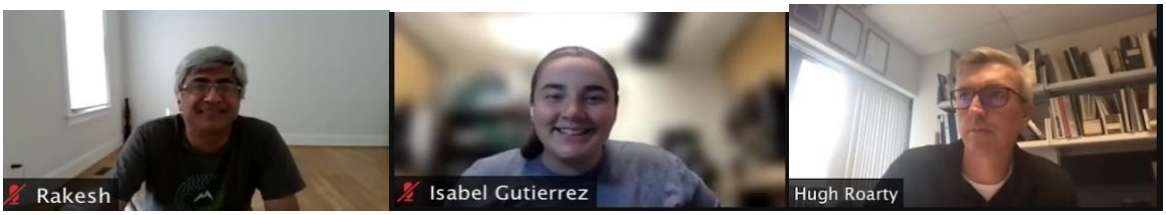



*Figure 3: Dr. Rakesh Malhotra and Isabel Gutierrez from NCCU participated in the SRI and collaborated with Dr. Hugh Roarty, Rutgers University, as part of the DHS Minority Serving Institution Summer Research Team program.*

The Risk Management & Analytics Dashboard built upon work conducted in the MSC's 2019 and 2020 SRI programs. This summer's project aimed to build a data visualization dashboard using ArcGIS/Esri software to better accommodate accessibility and usability by USCG Sector NY. The interactive tool was developed to conduct trend analysis of Marine Information for Safety and Law Enforcement (MISLE) incident data. The dashboard visualizes and displays data spatially and can be filtered to analyze reported maritime incidents over weekly, monthly, and annual timescales, as well as by incident type and subtype (e.g., incident: marine environmental protection, subtype: pollution-oil). The dashboard includes an interactive map created through a geographic information system (GIS) using ArcGIS online. The map uses multiple layers to effectively display USCG MISLE data spatially and in graph and chart formats and updates as the data display is changed using various filters. The filters can be combined and layered for more in-depth analysis of the data. The ArcGIS/Esri platform supersedes the Dashboard developed using Tableau software in the SRI 2020 program.

The team has developed a user-guide and is working to transition the tool for piloting by USCG Sector NY in late summer/early fall 2021. Figure 4 shows the ArcGIS/Esri interface and data display of the Risk Management and Analytics Dashboard.

The Dashboard project was led by Dr. Rakesh Malhotra from North Carolina Central University in conjunction with Geographic Information Systems master's degree student, Isabel Gutierrez as part of the DHS MSI Summer Research Team (MSI SRT) program. The team plans to apply for follow-on funding through the MSI SRT program to continue to build out the Dashboard for Sector NY and other USCG Sector Units.

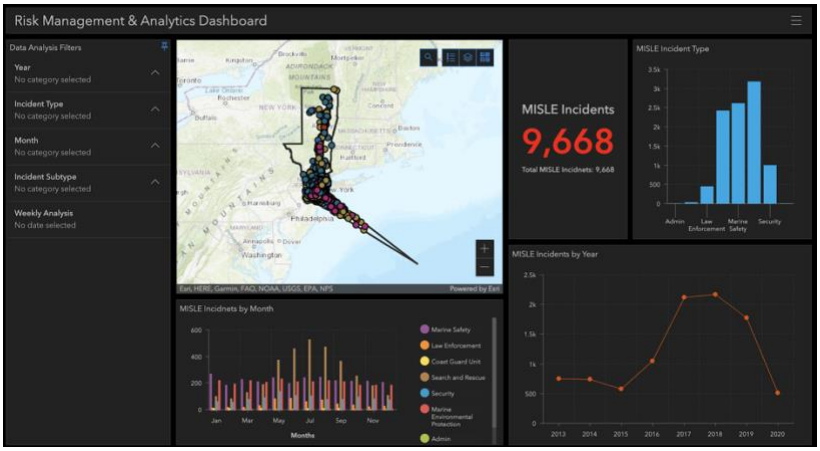



*Figure 4. The Risk Management and Analytics Dashboard graphically displays MISLE incident data for the USCG Sector NY AOR.*

A synopsis of the team's research, including the team's research question, importance to homeland security, methodology and outcomes are provided below in Table 6.

*Table 6. SRI 2021 – Risk Management and Analytics Dashboard Overview.*

| |
|---|
| **Project Title:** Risk Management and Analytics Dashboard |
| **Research Question:** *Do ArcGIS and Esri Dashboard create an interactive, easy-to-use visualization and data analysis tool for the USCG to display MISLE incident data?* |
| **Importance to Homeland Security:**<br>● The Risk Management Dashboard allows for quick visualization and an analytical perspective into incident trends.<br>● The tool will allow the USCG to be data driven and proactive in resource planning and allocation. |
| **Prospective End-user:** The Dashboard was customized and developed for USCG Sector NY. The framework for the visualization tool however, can be modified and used broadly across all USCG Sectors. |
| **Project Abstract:** The USCG Marine Information for Safety & Law Enforcement (MISLE) database is a national repository of all maritime incidents. The database is composed of incidents related to maritime safety, security, and marine environmental protection. There is a wide range of incident types recorded into this database from capsized vessels, collisions, and pollution to bridge closures, security breaches, and so on. This summer's research project utilized MISLE data for the USCG Sector NY and is a continuation of work conducted in the MSC 2019 and 2020 Summer Research Institute programs. This year's project uses ArcGIS and Esri software in lieu of Tableau software, to spatially display the MISLE incident data. The Dashboard is composed of a map, various graphs/charts, and filters for an array data. The Dashboard can be used to conduct incident trend analysis and will allow for enhanced planning and asset allocation. |
| **Approach/Methodology:**<br>The team developed an updated version of the Risk Management and Analytics Dashboard using ArcGIS and Esri software for better access and use by the USCG. |

| |
|---|
| Leveraging incident data received by Sector NY, the team parsed out and displayed data for the following categories.<br>● Geographical area<br>● Incident type and subtype<br>● Incident Time Scale |
| **Research Outcomes:** At the culmination of the SRI program, the team developed a working prototype of a dashboard visualization tool. A user guide has been developed and the Dashboard files are in the process of being transitioned to USCG Sector NY for the purposes of piloting the data visualization and analytics tool in late summer/early fall 2021. |

Additional details regarding the team's project can be found in their final research presentation slides, including a video recording of their presentation, and research poster located on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021. Table 7 below identifies the team members and their university affiliations.

*Table 7. Risk Management and Analytics Dashboard Team Members.*

| **Student** | **Academic Discipline** | **School** |
|---|---|---|
| Isabel Gutierrez | Geographic Information Systems | North Carolina Central University (NCCU) |
| **Faculty Mentors:** Dr. Rakesh Malhotra, Associate Professor, Environmental, Earth and Geospatial Sciences, NCCU and Dr. Hugh Roarty, Research Project Manager, Rutgers University | | |

**Research Team/Project: <u>BlueROV</u>**

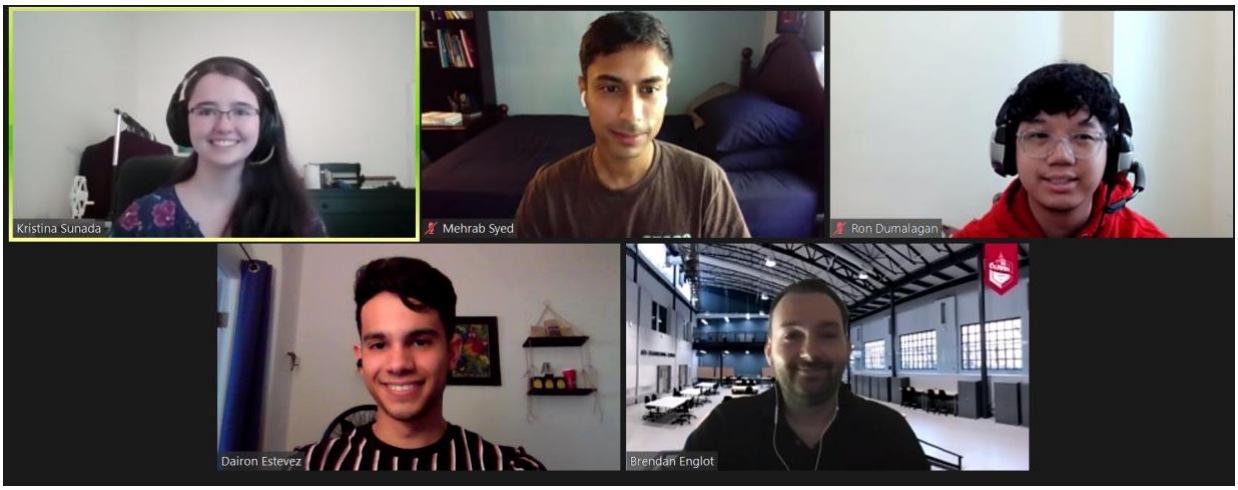



*Figure 5. Students on the BlueROV team worked to conduct a feasibility study and maritime security use cases for a custom built ROV with robotic arms.*

This summer's BlueROV research team was tasked with conducting a feasibility study to analyze the applications of robotic manipulator arms attached to a customized underwater remotely operated vehicle (ROV). The ROV is a modified version of the BlueROV2 Heavy Configuration sold by Blue Robotics. Manipulator arms are being developed for this ROV in order to expand the robot's uses for conducting high precision tasks. The goal for this project was to research and validate the potential uses of the ROV in regard to maritime security. The two main maritime tasks identified for the BlueROV to conduct are pier piling inspection, and Aids to Navigation (ATON) mooring chain inspection.

In order to explore the maritime tasks that were identified, the team created a mission planning tool. This tool was designed to allow the end user to predict how long it would take to complete a mission based on the number of ROVs and the requirements of the mission. This tool will also allow for the BlueROV to more efficiently be deployed for maritime security missions, including the inspection of ATON. As part of their research program, the students met with homeland security personnel from the USCG Sector NY, USCG Research and Development Center and Customs and Border Protection Port of NY/Newark to discuss use cases for the custom built ROV. Representatives from USCG Sector NY have offered to collaborate and conducted a deployment of the ROV during the latter part of the summer.

A synopsis of the team's research, including the team's research question, importance to homeland security, methodology and outcomes are provided below in Table 8.

*Table 8. SRI 2021 – BlueROV Overview.*

| **Project Title:** BlueROV |
|---|

**Research Question:** *Can robotic arms be used with the BlueROV to complete high-precision maritime security tasks autonomously?*

**Importance to Homeland Security:**
Underwater remotely operated vehicles, ROVs, have become more advanced with new technology such as 3D sonar reconstructions and manipulator arms. With this new technology, it is possible for ROVs to be used for high precision maritime security tasks such as pier piling inspection, and aid to navigation (ATON) mooring chain inspection. These two tasks are important for maintaining the health and safety of waterways, and by automating them with ROVs it could be more efficient and safer for all personnel involved.

**Prospective End-users:** USCG and CBP, among other homeland security stakeholders.

**Project Abstract:** The Stevens BlueROV is a remotely operated underwater vehicle (ROV) equipped with two imaging sonars and a monocular camera. This summer, the research team conducted a feasibility study to investigate the addition of robotic continuum manipulator arms to the modified BlueROV. The team was primarily interested in exploring the use of such arms for conducting high precision and energy-efficient maritime security tasks. The team met with experts in the field of Aid to Navigation (ATON) inspections and analyzed reports from local pier inspections. The team was then able to create a mission planning tool that used estimated speeds and battery usage to calculate the amount of time needed for different tasks. This tool is useful for estimating mission logistics, such as the numbers of ROVs required for a given mission. The two tasks addressed in the planning tool are pier piling inspection and ATON mooring chain inspection. Inspection of these two types of maritime infrastructure are important for public safety, along with the health of the waterways. In addition to the mission planning tool, simulations of the BlueROV with manipulator arms were created in order to demonstrate how the ROV would be able to grip onto the structures for better stability during inspection. By having the BlueROV conduct these inspections autonomously, the Coast Guard, MSC (Maritime Security Center), and other agencies could eliminate many of the risks associated with having divers inspect infrastructure. Further development of this technology could also lead to more time efficient and cost-effective missions.

**Approach/Methodology:**

- The team conducted a feasibility study to analyze the applications of robotic manipulator arms attached to a customized underwater remotely operated vehicle (ROV).
- The team created a mission design tool to show how feasible it would be for BlueROVs to complete missions given a set of parameters. This mission design tool was created as a spreadsheet so that the inputs can easily be changed to represent different scales and conditions for missions.

**Research Outcomes:** The outputs created from the mission design tool can be used to determine the feasibility of the missions and predict how long it will take to conduct the mission. The Battery Operational Time is calculated based on the power usage of the sensors, thrusters and manipulator arms. The Mission Operation Time is calculated based on the speed of the water currents, and the distance between pilings. If the Battery Operational Time is greater than the Mission Operation Time,

then theoretically the batteries on the ROV do not need to be recharged during the mission.

Additional details regarding the team's project can be found in their final research presentation slides, including a video recording of their presentation, and research poster located on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021. Table 9 below identifies the student team members, their academic disciplines and their university affiliations.

*Table 9. BlueROV Team Members.*

| **Student** | **Academic Discipline** | **School** |
|---|---|---|
| Ron Dumalagan | Computer Science | Stevens Institute of Technology |
| Dairon Estevez | Mechanical Engineering | Columbia University |
| Mehrab Syed | Software Engineering | Stevens Institute of Technology |
| Kristina Sunada | Mechanical Engineering | Stevens Institute of Technology |
| **Faculty Mentor:** Dr. Brendan Englot, Stevens Institute of Technology | | |

**Research Team/Project: <u>Hazardous Cargo Inspection</u>**


*Figure 6. Students on the Hazardous Cargo Inspection Team collaborated with Dr. Barry Bunin, Stevens Institute and USCG Sector NY to identify improved methods for targeting undeclared and misdeclared hazardous cargo.*

The Hazardous Cargo Inspection team was tasked with identifying improved methods for finding non-compliant cargo containers. The team's objectives were to find correlations between dangerous cargo and different predictive measures such as hazard type, and country of origin to develop improved processes for identifying and intercepting misdeclared, undeclared and mispackaged hazardous cargo. The team analyzed MISLE

data among other data sets provided by USCG Sector NY to determine high-risk cargo based on hazard type and failed inspection rates, among other variables.

The team met routinely with personnel from USCG Sector NY and had the opportunity to speak with members of the National Container Bureau and with personnel from Sector Virginia who also expressed interest and contributed to the project.

Outcomes from the team's research brought to light a number of data infirmities that thwarted a conclusive investigation of the cargo inspection data; however, the team were able to develop a preliminary algorithm that can be used by Sector NY to enhance their targeting and inspections of hazardous cargo. The team's research project has been brought to the attention of USCG HQ and has the potential for contributing to improved inspections nationally.

A synopsis of the team's research, including the team's research question, importance to homeland security, methodology and outcomes are provided below in Table 10.

*Table 10. SRI 2021 – Hazardous Cargo Inspection Team Members.*

| |
|---|
| **Project Title:** Improved U.S. Coast Guard Dangerous Cargo Container Inspections |
| **Research Question:** *How to increase success rate of finding non-compliant containers by targeting inspections for high-risk cargo?* |
| **Importance to Homeland Security:** The United States Coast Guard (USCG) is responsible for inspecting thousands of containers a year, but they are unable to inspect every container that comes into port. Some of these containers that the USCG are unable to inspect contain either mispackaged, misdeclared, or undeclared cargo. This can cause serious issues as they can cause structural issues where containers could fall into the sea or even onto ship workers. Even more seriously, this can cause cargo ship container fires. |
| **Prospective End-user:** USCG Sector NY, USCG HQ |
| **Project Abstract:** An increasing number of container ship incidents such as ship fires are found to be caused by misdeclared and undeclared hazardous cargo. Container ship incidents have cost more than 100 billion dollars in lost cargo, environmental damage, and fires due to misdeclared and undeclared hazardous cargo. Overlooking these concerns could lead to damage to the cargo and vessel and more importantly, loss of life. The United States Coast Guard (USCG) inspects thousands of containers in an attempt to minimize this issue, however the United States sees over 11 million containers in imports alone, leaving the USCG unable to inspect the majority. This project aims to increase the success rate of finding non-compliant containers by targeting inspections for high-risk cargo, by developing an algorithm that is able to calculate the risk a container poses based on its attributes. The student team analyzed data sets of past inspections performed by the USCG and utilized this data to predict high-risk containers that should be inspected more frequently in the future. The team will also examine container numbers included in the data sets and utilize container validity calculations to find fraudulent containers. The team developed a container number calculator that automatically returns whether a container number is valid or not. In addition, the team has noted limitations in the data that the Coast |

| |
|---|
| Guard did not notice in the past. The resulting algorithm will be able to process input parameters such as hazard class and country of origin and identify the risk factor based on historical data. |
| **Approach/Methodology:**<br>● The team utilized Microsoft Excel to perform research tasks.<br>● The team analyzed MISLE data provided by USCG Sector NY to identify different types of reported hazardous incidents, the USCG districts reporting the highest number of incidents and the cargo country of origin. |
| **Research Outcomes:** At the culmination of the SRI program, the team identified several data infirmities in need of remediation and developed a preliminary algorithm that USCG Sector NY can begin to pilot to more efficiently and effectively target potential high-risk cargo. |

Additional details regarding the team's project can be found in their final research presentation slides, including a video recording of their presentation, and research poster located on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021. Table 11 below identifies the student team members, their academic disciplines and their university affiliations.

*Table 11. Hazardous Cargo Inspection Team Members.*

| **Student** | **Academic Discipline** | **School** |
|---|---|---|
| Erin Harrison | Civil Engineering | Stevens Institute of Technology |
| Andrew Narvaez | Computer Science | Stevens Institute of Technology |
| Samantha Weckesser | Software Engineering | Stevens Institute of Technology |
| Xinyuan Luo | Applied Mathematics | Stevens Institute of Technology |
| **Faculty Mentor:** Dr. Barry Bunin, Stevens Institute of Technology | | |

**Research Team/Project:** ***Cybersecurity and Data Analysis – USCG Sector NY Internship***


*Figure 12. MSC summer research student Tara McLoughlin had the unique opportunity to conduct her cybersecurity research project in collaboration with Mr. John Hillin, Safety and Security Division Chief on-site at USCG Sector NY.*

Prior to the start of the 2021 SRI, Sector NY made available an internship opportunity focusing on cybersecurity and data analysis in the Port of NY/NJ. Through communication with Mr. John Hillin, Safety and Security Division Chief at Sector NY, a cybersecurity student within the SRI 2021 admitted student group was identified as a high-potential candidate. Working in conjunction with the student, Tara McLoughlin, the MSC and Sector NY developed a mutually agreed upon internship project that allowed Tara to apply her cybersecurity skills in a field-based internship with USCG Sector NY. Since starting her internship in May, Tara was able to observe USCG marine safety personnel conduct facility inspections and to participate in the inspection of a vessel following reports of a possible cyber breach. As part of her internship tasks, Tara reviewed cybersecurity plans, and met with terminal operators and maritime industry partners in the Port of NY/NJ to better understand their cybersecurity procedures and preparedness. At the end of her internship, Tara developed several documents to support Sector NY's cybersecurity initiatives, including a report on cybersecurity best practices, a cybersecurity checklist for marine inspectors, and recommendations for cybersecurity training programs.

Ms. McLoughlin was recognized by Sector NY for her efforts, at the USCG Area Maritime Security Committee Executive Steering Committee meeting held on August 10, 2021, at the Manhattan Marine Terminal in New York City.

A synopsis of Tara's summer internship project is provided below in Table 12.

*Table 12. SRI 2021 – Cybersecurity and Data Analysis – Internship Project Overview.*

| |
|---|
| **Project Title:** Cybersecurity and Data Analysis Internship Project |
| **Research Question:** *How can the Coast Guard determine the adequacy of cybersecurity plans and proposals in the absence of prescriptive laws and regulations?* |
| **Importance to Homeland Security:** |

| |
|---|
| The U.S. Coast Guard has been tasked to ensure the safety and security of the Nation's ports, including the evaluation of cybersecurity plans. The research aimed to address how the Coast Guard can determine adequacy of cybersecurity plans and proposals in the absence of prescriptive laws and regulations. |
| **Prospective End-user:** USCG and maritime and port community partners. |
| **Project Abstract:** Cyber-attacks on critical infrastructure including maritime information and operational technology have greatly increased over the past few years. For example, four of the world's largest global maritime shippers (i.e., CMA CGM, MSC, Maersk, and Cosco) have been impacted by varying forms of malware and ransomware, causing losses of millions of dollars and disruptions to critical supply chains including the maritime transportation system (MTS). The U.S. Coast Guard is responsible for ensuring the safety and security of the Nation's ports and waterways, including protecting the MTS against cybersecurity threats. An intern in the Maritime Security Center's 2021 Summer Research Institute engaged in a field-based internship with USCG Sector New York, to analyze the Coast Guard's process and procedures for conducting cybersecurity assessments. These assessments are a part of the Maritime Security Transportation Act (MTSA)-required facility and vessel security plans, as well as the USCG's cyber incident response efforts. The internship included accompanying Sector NY marine safety personnel on facility inspections, reviewing maritime facility cybersecurity plans, and observing the Sector's response to a suspected cyber breach on a vessel. Outcomes from the student's internship included the development of a cybersecurity assessment checklist for Coast Guard marine inspectors, a list of basic and best cybersecurity practices for maritime facility operators, and fundamental education and training recommendations for small and mid-sized maritime operators. |
| **Approach/Methodology:**<br>● Work with Coast Guard operators to assess the process and procedures for conducting cyber reviews and assessments<br>● Review and assess adequacy of cyber assessment documents<br>● Gain a background perspective on the Coast Guard and how it has worked to maintain physical security<br>● Discuss cybersecurity approaches with Facility Security Officers<br>● Conduct field-based assessments and investigate cyber incidents |
| **Research Outcomes:** The following documents were created and provided to USCG Sector NY for their use:<br>● Cyber Training Document to assist in cybersecurity training at facilities.<br>● Facility Vulnerability Measures document to establish possible cyber threats.<br>● A Sample Cybersecurity Facility Security Plan that can be used as an example for facilities to base their own cyber plans.<br>● Suggestions for MARSEC regulation updates to include cybersecurity.<br>● A Marine Inspections Checklist was developed, and was beta tested at three facilities. |

Additional details regarding the Cybersecurity and Data Analysis internship project can be found on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-

training/summer-research-institute/sri-2021. Table 13 below identifies the student team member, their academic disciplines and university affiliation.

*Table 13. Cybersecurity and Data Analysis Internship Project.*

| **Student** | **Academic Discipline** | **School** |
|---|---|---|
| Tara McLoughlin | Cybersecurity | Stevens Institute of Technology |
| **Faculty Mentor:** Dr. Barry Bunin, Stevens Institute of Technology and Mr. John Hillin, Safety and Security Division Chief, USCG Sector NY | | |

### 3.2.9 SRI 2021 Student Survey

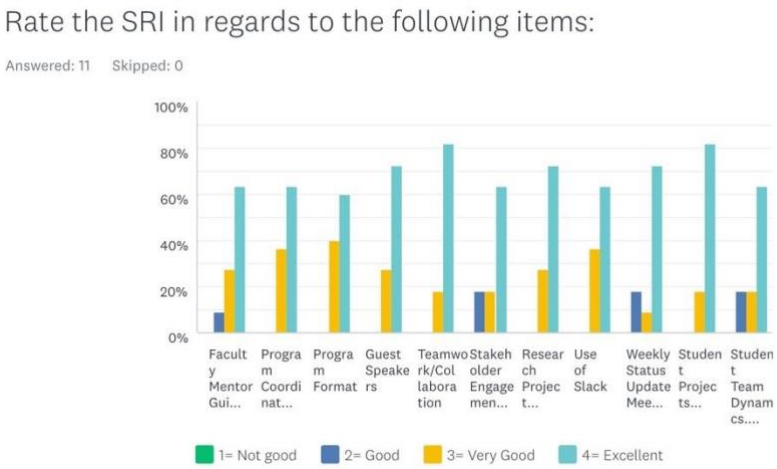



*Figure 8. SRI student survey respondents rated the SRI "Excellent" in all categories in a post-program survey.*

An assessment of the 2021 summer research program was conducted via a student survey (see Appendix E-1 for a copy of the student survey questions and format). Student participants were each asked to complete an online survey and to provide feedback on the virtual delivery of the summer research program, the students' learning gains, areas for program improvement and program impacts on student interest in advanced study and/or careers in homeland security. The survey was completed by 11 of the 14 student participants.

A majority of the student respondents rated the SRI Excellent in all categories, including the following:

- Teamwork/Collaboration (82%)
- Student Project Assignment (82%)
- Research Project Outcomes (73%)
- Guest Speakers (73%)
- Program Format (73%)

- Weekly Status Update Meetings (73%)
- Faculty Mentorship (64%)
- Stakeholder Engagement (64%)
- Program Coordination/Administration (64%)
- Student Team Dynamics (64%)
- Use of Slack (64%)

100% of the survey respondents stated that the SRI enhanced their interest in advanced academic study and careers in the homeland security domain, and 100% of the students reported that they would recommend the program to their peers and colleagues at their respective schools.

When asked to what extent the SRI enhanced or improved their skills, a majority of the students reported “Significant Improvement” in the following areas:

- Communication Skills (82%)
- Ability to Conduct Research (73%)
- Leadership Skills (73%)
- Oral Presentations (73%)
- Professional Confidence (73%)
- Self-Motivation (73%)
- Teamwork/Collaborations (64%)
- Organizational Skills (64%)
- Networking (55%)

When asked to describe their experience in the virtual SRI and identify their “top takeaways”, the students commonly mentioned the following:

- Developed research skills and professional experience.
- Insight and knowledge into maritime security
- Collaboration and communication with stakeholders

When asked to identify the strengths and weakness of the program, students frequently mentioned the following:

Strengths:

- Program environment, collaboration and feeling of community.
- Interactions with stakeholders.
- Student independence and ownership of research outcomes.

Weaknesses:

- Need more opportunities for the entire student group to interact, not just in their respective teams.
- Students should be allowed to self-select their own research projects.

The students worked in collaboration with assigned researcher mentors and had the unique opportunity to interact and engage with homeland security practitioners throughout the summer research program. Through their experience in the summer research program, students gained a greater awareness of maritime and homeland security issues. Student survey responses show that participation in the SRI has effectively inspired student interest to pursue careers and academic study in the homeland security domain. Collectively, the SRI was effective in achieving the following outcomes:

- MSC stakeholders requested briefings and materials on the student research team projects.
- Each of the five student teams will submit their research posters for consideration to the 2021 Maritime Risk Symposium.
- Student presentations and research reports demonstrated that the students gained knowledge and understanding of the maritime security domain and their respective research projects.
- A majority of the students (100%) expressed enhanced interest in pursuing careers and/or advanced academic study in maritime/homeland security as a result of their participation in the SRI.

## 3.3 Graduate and Undergraduate Research Assistantship Programs

### 3.3.1 Milestones and Metrics

| # | Milestone | Performance Metric | Output |
|---|---|---|---|
| M1 | Prospective student outreach and recruitment (7/1/2020 – 8/31/2020) | Confer two Master's degree-level Research Assistantships. | Completed: MSC awarded two one-year Research Assistantships. |
| M2 | Students complete requisite course work/research. (8/31/20 – 5/28/21) | Research Assistants maintain GPA requirements and enroll full-time in coursework. Research Assistants engage in up to twenty hours of MSC research per week during the fall and spring semesters | Completed: The students were enrolled full-time and met all GPA and weekly research requirements for the 2020/2021 academic year. |
| M3 | Students present research at MSC event or related DHS/stakeholder event. (3/1/21 – 6/30/21) | Students complete research reports and/or thesis based on research completed. | Completed: The students presented their research to MSC researchers and participated in the 2021 COE |

| | | | |
|---|---|---|---|
| | | | Summit. One student was awarded 1st place best student poster at the Summit. |

### 3.3.2 MSC Research Students

Five students conducted research with the MSC throughout the 2020/2021 academic year (Year 7). The students included two graduate students who participated in the Center's Graduate Research Assistantship program and three undergraduate students who assisted with MSC research tasks as Research Support Assistants. The graduate students were provided funding support through the MSC and the undergraduate students were provided stipend support by Stevens Institute of Technology. Table 14 below provides an overview of the students and their research activities.

*Table 14. MSC Research Students – Graduate and Undergraduate.*

| Student | Award / Program | Research /Activities |
|---|---|---|
| **GRADUATE STUDENTS** | | |
| Jonathan Adamson | Graduate Research Assistantship / Chemistry and Nanotechnology | Conducted research in the area of fentanyl detection methods and provided support to advance the Sulfur Emission Detection sensing platform created during the MSC's SRI 2020 program. |
| Ethan Jones | Graduate Research Assistantship / Computer Engineering and Software Engineering | Conducted research to assess visualization and data analytics platforms to display maritime data. Assisted in building out work conducted on the Risk Assessment and Predictive Analytics Dashboard developed during the SRI 2019 and 2020 programs. |
| **UNDERGRADUATE STUDENTS** | | |
| Domenico Albarella | Undergraduate Research Support Assistant/ Mechanical Engineering SRI 2018/SRI 2020 program alumni | Assisted in setting up protocols to allow MSC's FLIR camera feeds to be shared with USCG Sector NY. |

| | | |
|---|---|---|
| Gil Austria | Undergraduate Research Support Assistant/ Computer Science SRI 2020 program alumni | Provided coding support to assist in the development of a data visualization tool using Microsoft Power BI. |
| Connor Smith | Undergraduate Research Support Assistant/ Systems Engineering SRI 2020 program alumni | Provided support in transitioning the Risk Management and Data Analytics Dashboard created during the SRI 2020 into Microsoft Power BI. |

### 3.3.3 Graduate Research Assistants

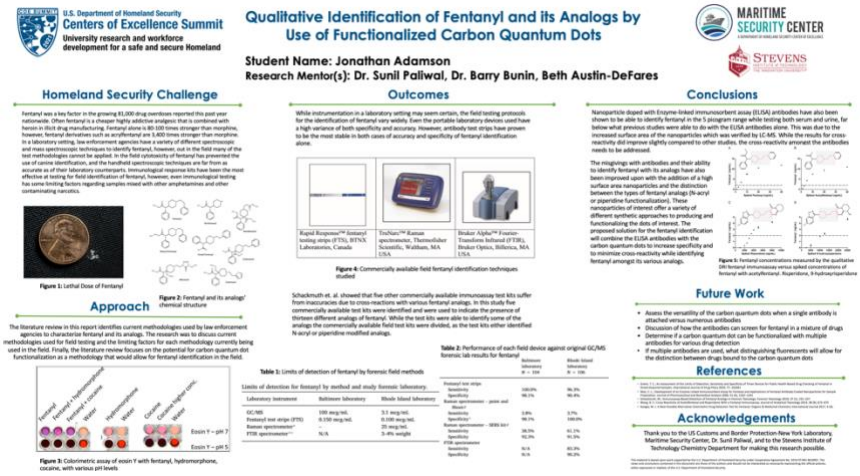



*Figure 9. MSC Graduate Research Assistant Jonathan Adamson was awarded 1st Place Best Student Poster at the 2021 COE Summit.*

The MSC Research Assistantship program engages graduate students in homeland security focused research projects resulting in technology development, research reports and/or master's theses. The research projects conducted in the Assistantship program are directly connected to current and emerging concerns in the maritime and homeland security domain. The homeland security-focused Assistantship program provides for full-tuition support, a monthly stipend and robust networking and field-based opportunities within the homeland security enterprise.

At the start of the 2020/2021 academic year, the Center conferred two graduate Research Assistantships to Ethan Jones (Computer Engineering/Software Engineering) and Jonathan Adamson (Chemistry/Nanotechnology). The Assistantships were conducted remotely due to the COVID pandemic. The Stevens Institute of Technology students were competitively selected to participate in the virtual program based on their research interests, academic standing and faculty recommendations.

As part of their program requirements, the students were enrolled fulltime and conducted twenty hours per week in research activities.

**Jonathan Adamson**

Jonathan Adamson served as an MSC Graduate Research Assistant during the Center's Year 6 (2019/2020 academic year) and was awarded a second assistantship in Year 7. During his assistantship program, Jonathan continued to investigate new methods for efficiently and effectively detecting fentanyl and its derivatives, and also provided research support to further develop the sulfur emission detection sensing platform developed in the MSC's 2020 Summer Research Institute.

Over the course of the academic year, Jonathan completed 18 credits towards the balance of his master's degree requirements and presented his research in a poster competition held during the 2021 COE Summit. During his Assistantship, Jonathan engaged in the following courses and fellowship/research activities.

| Semester | Course Title | Credits |
|---|---|---|
| Fall 2020 | CH 640 Adv Organic & Heterocyclic Chem | 3 |
| Fall 2020 | CH 660 Advanced Instrumental Analysis | 3 |
| Fall 2020 | CH 800 Special Research Problems in Chemistry | 3 |
| Spring 2021 | CH 800 Special Research Problems in Chemistry | 3 |
| Spring 2021 | CH 520 Advanced Physical Chemistry | 3 |
| Spring 2021 | Bio 800 Special Problem in Biology | 3 |

Assistantship/Research Activities:

- Conducted 20 hours per week of research.
- Provided research support to the MSC and Dr. Bruce Kim, City College of New York, as part of the MSI Summer Research Team follow-on funding for the Sulfur Emission Detection project developed during the MSC's 2020 SRI program.
- Attended virtual bimonthly meetings with MSC and Stevens faculty mentors.
- Presented research in a poster competition held May 18, as part of the 2021 COE Summit.
- Awarded 1st Place Best Student Poster Award at the COE Summit

**Ethan Jones**

Ethan Jones was selected to participate in the Assistantship program to assist in analyzing different visualization and data analytics tools to best display and analyze maritime data for the MSC stakeholders.

Over the course of the academic year, Ethan completed 18 credits towards the balance of his master's degree requirements and presented his research in bimonthly meetings with MSC researchers. During his Assistantship, Ethan engaged in the following courses and fellowship/research activities.

| Semester | Course Title | Credits |
|---|---|---|
| Fall 2020 | CPE 555 Real-Time and Embedded Systems | 3 |
| Fall 2020 | EE 551 Engineering Programming - Python | 3 |
| Fall 2020 | EE 695 Probability and Stochastic Processes 1 | 3 |
| Spring 2021 | CPE 517 Digital & Computer System Architecture | 3 |
| Spring 2021 | CPE 695 Applied Machine Learning | 3 |
| Spring 2021 | EE 608 Applied Modeling & Optimization | 3 |

Assistantship/Research Activities:

- Conducted 20 hours per week of research as part of the Assistantship program.
- Attended virtual bimonthly meetings with MSC and Stevens faculty mentors.
- Participated in the COE Summit Grand Challenge Tabletop Exercise event on May 18, 2021.
- Prepared documentation for a Risk Management Dashboard developed in Microsoft Power BI for MSC administrators.

Jonathan Adamson and Ethan Jones completed their degree requirements and were awarded master's degrees from Stevens Institute of Technology in May 2021. Both students are currently applying for positions within the homeland security space.

### 3.3.4 Undergraduate Research Assistants

During Year 7, Stevens Institute of Technology provided funding support for three undergraduate students to provide research support to the Maritime Security Center. The students were alumni of the MSC's Summer Research Institute program. The tasks and research activities of the MSC undergraduate research assistants were described above in Table 14.

## 3.4 MSI Engagement Workshop

### 3.4.1 Milestones and Performance Metrics

| # | Milestone | Performance Metric | Output |
|---|---|---|---|
| M1 | Development of workshop topic and curriculum (7/1/20 – 12/30/20) | Workshop topic to be determined by MSC and DHS stakeholders. | Completed: MSC discussed potential workshop topics |

| | | | |
|---|---|---|---|
| | | | and modules with its USCG partners from Sector NY and USCG First District. |
| M2 | Workshop held (3/15/2021 – 5/30/2021) | Workshop participation will include MSI and Community College educators and DHS stakeholders<br><br>Workshop attendees will include representations from a minimum of three MSI schools and community colleges.<br><br>A minimum of one DHS stakeholder representative will participate in the workshop event. | Completed: MSC held the workshop virtually on April 30, 2021. Representatives from four MSI schools attended, including four homeland security professionals representing the Coast Guard Academy, USCG First District, USCG Sector NY, and DHS S&T. |

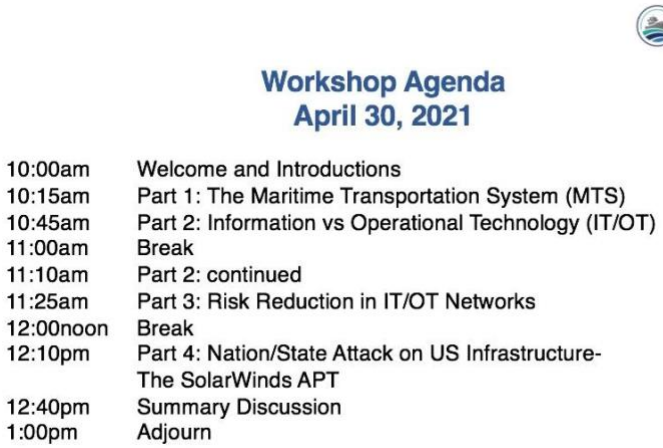



*Figure 10. MSC's 2021 MSI Workshop was held virtually, and included educators from Norfolk State University, New Jersey City University, Texas Southern University, and Florida International University.*

### 3.4.2 MSI Workshop

The MSC held a virtual workshop for faculty members from Minority Serving Institutions (MSIs) on April 30, 2021. The workshop aimed to build greater awareness of the maritime domain as a key component of the U.S. critical infrastructure system and to provide educators from a broad base of academic disciplines with an understanding of the

vulnerabilities of the Maritime Transportation System (MTS), and the key roles that both Information Technology and Operations Technology play.

The workshop leveraged curriculum developed by Stevens Institute of Technology and the Maritime Security Center in conjunction with Coast Guard Cyber Command.

The workshop was led by Dr. Barry Bunin, Research Professor at Stevens Institute of Technology and included conversations with USCG representatives from the Coast Guard Academy, USCG Sector NY and USCG First District, on the U.S. Coast Guard's cyber initiatives and workforce imperatives.

Workshop attendees included faculty and program directors from Florida International University, New Jersey City University, Norfolk State University, and Texas Southern University, in addition to the DHS stakeholders mentioned above.

The curriculum for the virtual event included the following modules:

Part 1: The Maritime Transportation System (MTS)
- Structure and Architecture
- Physical and Cyber Vulnerabilities
- Case Study: Maersk and NotPetya

Part 2: Information vs Operational Technology (IT/OT)
- Critical Infrastructure and Kinetic Harm
- Vulnerabilities and the Patching Dilemma
- Case Study: The Stuxnet Virus and Nation/State Threat Actors

Part 3: Risk Reduction in IT/OT Networks
- Privilege Management
- Firewalls and Demilitarized Zones (DMZ)
- Case Study: Critical Infrastructure-Pipeline Attack

Part 4: Nation/State Attack on US Infrastructure- The SolarWinds APT
- Analysis of the Attack
- Remediation and Ongoing Measures
- Discussion: Research Opportunities

To assess the effectiveness of the workshop in providing relevant and useful curriculum development information, the MSC asked the participants to complete a post-workshop survey. (See Appendix E-2 for copy of the survey instrument). Six out of the nine participants completed the workshop survey. When asked what inspired them to attend the workshop, the respondents commonly reported the relevance of the topic to their academic programs, the desire to learn new topics and incorporate new curriculum into their classrooms, and the opportunity to network with colleagues from other schools. When asked if the workshop content met their expectations, 50% said that the workshop "Exceeded My Expectations", and 50% said that the workshop "Met My Expectations". The quality of the workshop was rated Excellent in all of the following categories:

- Quality of Workshop Curriculum (67%)
- Quality of Instruction (67%)
- Participation Engagement and Dialogue (67%)
- Quality of Workshop Coordination Administration (83%)
- Ease of Online Platform (50%)

When asked how they would improve the workshop for future participants, some suggested a future in person event, and another recommended creating a centralized repository for maritime cybersecurity resource materials.

MSC continues to stay in communication with the MSI Workshop participants via email and has shared several opportunities for collaboration and engagement as they pertain to the DHS MSI Summer Research Team and HS-Power programs, among other relevant programs of interest.

## 3.5 DHS MSI Summer Research Team

MSC hosted DHS MSI Summer Research Teams from Norfolk State University (NSU) and North Carolina Central University (NCCU) during Year 7. The NSU team included Dr. Mary Ann Hoppa, Associate Professor, Norfolk State University, and undergraduate students Tricia Camaya and Zaid Abdul-Kaudeyr, and the NCCU team included Dr. Rakesh Malhotra, Associate Professor, Environmental, Earth and Geospatial Sciences, and master's degree student Isabel Gutierrez. Both team's research projects were held virtually in conjunction with the MSC's Summer Research Institute.

Dr. Hoppa and her team's research project focused on assessing the cybersecurity risks associated with offshore wind farms, and Dr. Malhotra's team worked to develop data visualization dashboard using ArcGIS.

Details regarding the MSI Summer Research Team's research projects and outcomes can be found in the Summer Research Institute section of this report, in Section 3.3.8, and on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/summer-research-institute/sri-2021.

## 3.6 Maritime Cybersecurity Professional Development Course

PI: Beth Austin-DeFares and Dr. Barry Bunin, Stevens Institute of Technology
Project Period: July 2020 - June 2021

### 3.6.1 Overview and Objectives

MSC research PIs Beth Austin-DeFares and Dr. Barry Bunin, from Stevens Institute of Technology have collaborated with Coast Guard Cyber Command and USCG Sector NY, since 2019 to develop a Maritime Cybersecurity professional development course tailored to the education needs of USCG marine safety personnel. The two-day, instructor-led course was created to provide a baseline understanding of cybersecurity concepts and an increased awareness of cybersecurity vulnerabilities and mitigations to assist Coast Guard personnel in making cyber assessments as part of facility and vessel inspections and incident response efforts. The professional development course aims to build capacity in cybersecurity knowledge within the context of the maritime domain and to support the Coast Guard's cybersecurity workforce imperatives.

The MSC piloted the course for USCG LANTAREA personnel on October 1 and 2, 2020, and for PACAREA personnel on December 3 and 4, 2020. The courses were held virtually due to the COVID pandemic.


*Figure11*. Representatives from nine sector units in PACAREA participated the MSC's Maritime Cybersecurity Professional Development course held virtually December 3 & 4, 2020.

### 3.6.2 Project Milestones and Performance Metrics

| # | Milestone | Performance Metric | Output |
|---|---|---|---|

| | | | |
|---|---|---|---|
| M1 | Collaborate with USCG Cyber Command to assess feedback received from the pilot course. (9/15/20 – 12/30/20) | Refine professional development short course based on CG Cyber and participant survey. feedback. | Completed: MSC prepared summary reports for CG Cyber Command and USCG HQ, including participant survey feedback for both the LANTAREA and PACAREA pilot courses. Adjustments to the PACAREA course were made based on feedback from the LANTAREA pilot. |
| M2 | Flesh-out and modify curricula, course delivery format, and prospective audience to further meet Coast Guard Cyber education needs and those of the maritime industry. (9/15/20 – 12/30/20) | | Completed: MSC has developed a course proposal tailored to USCG personnel. |
| M3 | Identify collaborators/transition partners for future ownership and delivery of the course content. (10/1/20 – 1/30/21) | Engage in a minimum of five curriculum discussion and development meetings with USCG POC and prospective transition partner. | Partially Completed: Following the LANTAREA course, MSC met with the POC from CG Cyber Command to host an additional course for PACAREA personnel. In lieu of transitioning the course to a collaborator following the PACAREA course, the MSC prepared a proposal to extend the MSC's |

| | | | |
|---|---|---|---|
| | | | ongoing delivery of the course. A transition partner will be identified during Year 8 of the Center. |
| M4 | Map out curriculum, delivery, scalability and program cost structure and transition with prospective transition partner/collaborator. (10/1/20 – 4/30/21) | Prepare a report on the course curriculum, delivery format, prospective scalability of the course, the program cost structure and transition plan. | Completed: The MSC prepared a project proposal for its ongoing delivery of the course. The proposal was awarded and the MSC has been given an additional year to turn the course into a self-sustaining course offering. |
| M5 | Plan and confirm next course date and location with transition partner and CG Cyber. (10/1/20 – 4/30/21) | | Partially completed: MSC has proposed course dates for the fall of 2021 and the spring of 2022. The identification of a suitable transition partner has been postponed until Year 8. |

### 3.6.3 Maritime Cybersecurity Professional Development Pilot Course – Planning and Delivery

A course planning committee was formed to include representatives from the MSC, Coast Guard Cyber Command and Sector NY, to provide insight into Coast Guard policy, pertinent maritime cyber security areas for instruction, and relevant case studies and areas of interest to marine safety personnel and facility inspectors. The pilot course was scheduled to be held in April 2020, however, due to the COVID-19 pandemic, the course was postponed to October 1 and 2, 2020 and held remotely.

The course included 13 marine safety personnel representing nine Sectors from five different USCG Districts, including Sector New York, Sector Delaware Bay, Sector Maryland/National Capital Region, Sector New Orleans, Sector San Juan, Sector Sault St.

Marie, Sector Savannah, Sector Upper Mississippi River and Sector Virginia. The course also included 19 class observers from CG Cyber Command, CG-FAC, USCG Sector NY, and the USCG Auxiliary Cyber Task Force. RADM Michael Ryan, CG Cyber Command, CDR Brandon Link, CG-FAC and CAPT Jason Tama, Commander Sector NY provided remarks.

Following the success of the Atlantic Area pilot course, the planning committee organized a second pilot course to be held virtually December 3 & 4, 2020 for PACAREA. RADM Michael Ryan and Captain Rebecca Ore, Sector Commander, USGC Sector Los Angeles-Long Beach provided opening remarks. Student participants included 21 PACAREA marine safety personnel representing four Districts and nine Sector units.

Course summary reports and participant feedback surveys were conducted for each of the pilot courses and shared with USCG Cyber Command and with USCG HQ. Outcomes from the feedback survey are reviewed below in Section 3.6.4.

### 3.6.4 Course Modules and Delivery Format

The Maritime Cybersecurity professional development course is comprised of five modules. The sequence is designed to provide context on the Maritime Transportation System (MTS) as a key component of the Nation's critical infrastructure, and then offers a progression of topics to build participant understanding and knowledge of cybersecurity concepts and terminology, vulnerabilities, and mitigation strategies in Information Technology (IT) and Operational Systems (OT), and insight into cyber-attack methodologies used by perpetrators of recent cyber-attacks. Student participants receive certificates of participation and 1.3 Continuing Education Units (CEUs). The course modules include the following:

- **Module 1 - The Maritime Transportation System – Structure, Architecture, and Vulnerabilities -** This module includes three parts. Part 1 reviews the structure of the Maritime Transportation System (MTS), its components and its physical and cyber vulnerabilities. Part 2 introduces the basic concepts of Safety and Security, both Physical and Cyber. Concepts of Information and Operational Technology are introduced, and the importance that each of these play in the vulnerability of critical infrastructure, and in particular, the MTS. In Part 3, cyber-attacks are reviewed, including the vulnerabilities that were exploited and the mitigations proposed.

- **Module 2 - Fundamental Cyber Security and Tools**
  In Module 2, the dimensions of cyber security protection are introduced in terms of Confidentiality, Integrity and Availability of systems and infrastructure. Frequent attack vectors are discussed, as well as basic mitigation tools including authentication and access control.

- **Module 3 - Vulnerabilities and Risk Improvement in IT & OT**
  Historically, IT and OT infrastructures were considered separate entities. However, advances in technical complexity and requirements for increased efficiency have resulted in them being networked together. This, in turn, brings new cyber

vulnerabilities to the IT/OT infrastructure. In this Module, vulnerabilities due to networking and, in particular, remote access are introduced. These vulnerabilities can be mitigated through the use of concepts and systems such as firewalls, network segmentation and segregation, and demilitarized zones, which are discussed.

- **Module 4 - Cyber-Physical Risk Assessment and Security Issues in Cloud Computing**
  In this module, the risk management process and the concepts of Consequences, Vulnerability, and Mitigation are introduced. These concepts are fundamental to Risk Assessment/Risk Management Plans. These plans are the basis of Facility Management Plans, as addressed in NVIC 01-20, *"Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities"*. Next, the concept of cloud computing is introduced and how it might be approached for use in the MTS as a capability as well as a risk management tool.

- **Module 5 - GPS and AIS: Operation, Jamming, and Spoofing**
  In this module, GPS and AIS operations are presented. Jamming and Spoofing attacks are discussed, as well as recent exploits.

### 3.6.5 LANTAREA Pilot Course Feedback

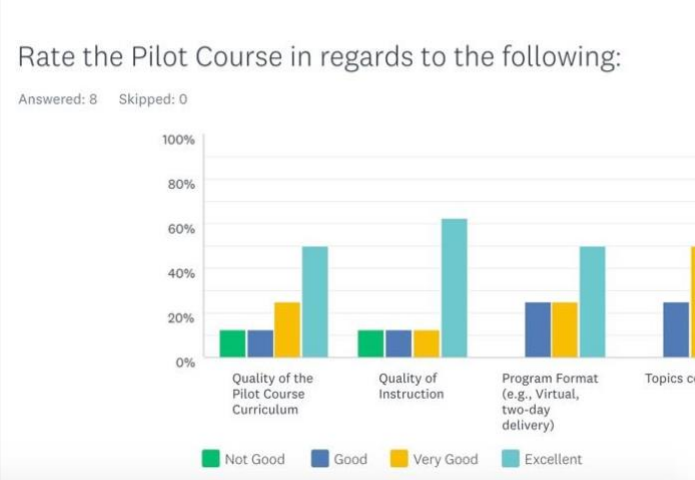



*Figure 11. A majority of the LANTAREA pilot course survey respondents rated the course "Excellent" in Quality of Curriculum, Instruction and Format.*

A post-program survey was distributed for both the Atlantic Area and PACAREA pilot courses. For the Atlantic Area, eight out of the 13 student participants completed the survey. Overall, the course assessments were very positive. A majority of the participants rated the course "Excellent" *in the Quality of the Curriculum (50%), the Quality of Instruction (63%) and in Program Format (50%).*

When asked if the course had met their expectations, a majority of the survey respondents (50%) said that "*the course had met my expectations and will be useful to my job*", and

12% said that "*The course curriculum/content Exceeded my expectations and will have a positive impact on my job."*

A separate survey was also conducted for the class observers. For the Atlantic Area course, nine out of the nineteen observers completed the survey. A majority of the observers (89%) said that they observed the class because "*the course was important to the education and training of my organization",* and 67% said that the "*course is important, and I am interested in working with the Maritime Security Center to develop more courses in this field*."

Overall, 56% of the Atlantic Area observers said that the course had met their expectations and had provided useful information, and 22% said that the course content had exceeded their expectations.

Following the course, the Planning Committee convened a meeting to include members from CG-FAC. The purpose of the meeting was to discuss the course survey feedback and lessons learned, and to plan for a future delivery of the course for PACAREA personnel. CG Cyber Command and CG-FAC assumed responsibility for the outreach and the coordination of the student attendee list for the PACAREA course. It was agreed that the course description be modified to ensure that the prospective participants understood that the course was intended to be a professional development course in cybersecurity concepts and foundational knowledge, and not a training course on how to conduct field-based cyber assessments.

### 3.6.6 PACAREA Pilot Course Feedback

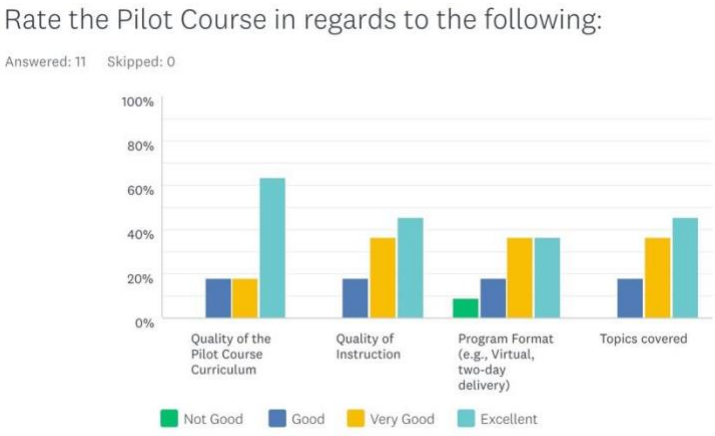



*Figure 12. A majority of the PACAREA pilot course survey respondents rated the course "Excellent" in Quality of Curriculum, Instruction, Format and Topics Covered.*

A post-program survey was distributed to the PACAREA student participants via Survey Monkey. Eleven out of the 19 participants completed the survey. Overall, a majority of the participants rated the course "Excellent" *in the Quality of the Curriculum (64%), the Quality of Instruction (45%) and in the Topics covered (45%).*

When asked if the course had met their expectations, 63% of the respondents said that the course curriculum/content had “exceeded their expectations and will have a positive impact their job”.

When asked how the course could be improved for future Coast Guard delivery, participants shared the following:

- *Provide additional guidance and/or information specific to the Coast Guard members' working needs. The duties of a facility inspector will undoubtedly become more fixated on cyber security measures as time goes on.*
- *More emphasis on the mission execution: NVIC 01-20 implementation, FSP expectations and examples.*
- *I think that some of the pacing of the course could be improved. While there was a lot of excellent material that was presented, there were a few things that could have been cut for time.*

A separate survey was also conducted for the class observers. Nine out of the nineteen observers completed the survey. A majority of the observers (100%) said that they observed the class because “*the course was important to the education and training of my organization”,* and 11% said that they were looking for new ways to keep my organization up to date in the field of cyber security.

Overall, 67% of the observers said that the course had met their expectations and had provided useful information, and 33% said that the course content had exceeded their expectations.

With regards to improving the course for future delivery, observer feedback included the following:

- *Add a section speaking to responsibilities (Sector, District, etc.) in responding to a cyber-attack/ notification of a cyber-attack on a facility/vessel.*
- *Ensure discussions on current cyber incidents and lessons learned are facilitated among inspectors.*

### 3.6.7 Ongoing Course Delivery

According to the 2020 National Maritime Cybersecurity Plan “*Federal maritime cybersecurity forces exist, but are not sufficiently staffed, resourced, and trained to monitor, protect, and mitigate cyber threats across the maritime sector”.* To address these workforce concerns, the MSC proposed and was approved by DHS OUP to provide ongoing Maritime Cybersecurity education opportunities for Coast Guard personnel, as well as USCG Area Maritime Security Committee (AMSC) members, and other relevant maritime sector groups to receive fundamental cybersecurity education within the context of the maritime domain.

The online professional development program will be sustained through a per person enrollment cost and will strive to develop pathways into degree granting programs,

including Stevens Institute of Technology's proposed Maritime Cyber Security Graduate Certificate program.

Course dates have been tentatively planned for Fall 2021 and Spring 2022. Stevens Office of Continuing and Professional Education will assist in coordinating the ongoing delivery of the course.

# 4 Communications and Outreach

The following Communications and Outreach activities were performed during Year 7.

Stakeholder Meetings and Engagement – MSC personnel have participated in multiple meetings with the USCG, including meetings with the research project champions and USCG HQ personnel. These activities have included Coast Guard engagement in the Summer Research Institute student research projects and final presentations event (i.e., Research and Development Center, Sectors NY and Sectors VA), USCG Atlantic Area and Pacific Area participation in the Maritime Cyber Security Pilot courses, and MSC research project review meetings (VTS Radar for Small Vessel Detection, Safety and Security of Remote Bridge Operations, and Low-Cost Covert Sensors for Remote Locations).

The Center's researchers and students also participated in the Maritime Risk Symposium (Oct. 26 – 30), at which, two of the MSC's SRI student research teams were awarded 1st and 2nd place Best Student Poster awards.

MSC's director continues to serve as an appointed member of the National Maritime Security Advisory Committee (NMSAC) and attended NMSAC virtual meetings.

MSC is actively engaged in DHS OUP COE activities, including participation on the Communications Working Group, Director's and Workforce Development Reps Calls, and assisting in chairing the COE Summit Education Committee. MSC also hosted two DHS MSI Summer Research Teams.

The MSC distributes a monthly update newsletter targeted to its DHS stakeholders. The Center's monthly updates are sent to more than 300 DHS and USCG stakeholder contacts, with new contact names being added to the distribution list as they arise. The Center maintains an archive of its newsletters on the Center website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/center-newsletters.

# 5 Other Related Activities

This section describes additional activities related to MSC that occurred during the reporting period. These include the Center's activities for soliciting projects, stakeholder engagement, communications and outreach, management, and guidelines and policies.

## 5.1 Project Solicitation

In Year 7, the MSC continued to leverage its network to solicit new projects. MSC conducted multiple meetings with the USCG representatives from various organizations, mainly from the Acquisition Directorate (CG-9) and from the Capabilities Directorate (CG-7) and from Customs and Border Protection Air and Marine Office. These meetings resulted in identifying a supplemental project with DHS S&T related to the efficacy of RF and acoustic sensors for autonomous applications. This project was completed in Year 7, where a final report was provided to DHS. Due to the COVID-19 pandemic, travel was restricted during Year 7 which limited our ability to meet with key stakeholders and pursue additional funding.

## 5.2 Stakeholder Engagement, Communications, and Outreach

MSC continued to engage partners from various key stakeholder organizations in a range of activities (e.g., Meetings, COE Summit, and Workshops). MSC personnel participated in numerous activities and partnered with the USCG HQ, USCG RDC, USCG Sector NY, DHS S&T Borders and Maritime Division, Customs and Border Protection Office of Field Operations, CBP New York Laboratory, National Urban Security Technology Lab, and others as described below.

### USCG HQ

Through a coordinated effort with DHS OUP, representatives from MSC met several times with USCG representatives from the Acquisition and Capabilities Directorates as well as representatives from different areas in the USCG, including the Living Marine Resources Enforcement Policy, Sector Corpus Christi, and Office of Bridges Programs. The meetings were very productive and resulted in fruitful discussions of the USCG needs.

In addition, the MSC Director is serving as a member of the National Maritime Security Advisory Committee (NMSAC) that is chaired by USCG CG-FAC members to provide technical advice to the USCG Commandant. The NMSAC met a couple of times, virtually during Year 7 and discussed high priority issues to the USCG.

### USCG RDC

USCG RDC provided a guest webinar during the MSC's 2021 Summer Research Institute titled Coast Guard UxS Discussion from Big Picture Strategy to Port Subsurface Capabilities Development and provided feedback on Coast Guard use cases for the BlueROV project. In addition, Ms. Grace Python, Operations Analyst and former MSC fellowship student participated as a panelist on the Finding a Place in the Homeland Security Workforce panel as part of the virtual COE Summit.

### USCG Sector New York

MSC and the USCG Sector New York collaborated over the past year to develop research project topics for the Center's 2021 Summer Research Institute. In addition to proposing projects, Sector NY's Safety and Security Division Chief, as well as several other Sector NY personnel participated as guest speakers, subject matters experts, and project mentors

during the SRI 2021 program. Outcomes from two of the summer research projects, the Risk Assessment and Analytics Dashboard and the Hazardous Cargo Inspections projects have been transitioned to Sector NY for piloting.

Sector NY also hosted an MSC summer research intern onsite for a ten-week cybersecurity internship project. The student was able to join Coast Guard personnel on facility and vessel inspections and assisted in developing several cybersecurity supporting documents for Sector NY.

MSC and Sector NY are also working together to identify eligible candidates for cybersecurity positions at Ft. Wadsworth. Throughout Year 7, MSC's Director of Education continued to serve as a co-Chair for the USCG Sector NY Area Maritime Security Committee – Cybersecurity Subcommittee.

**S&T Tech Centers**

MSC Director met on multiple occasions with DHS S&T Tech Center Subject Matter Experts to discuss sensors, unmanned platforms for maritime security, countering unmanned aerial systems, and Machine Learning applications in maritime and port security. These discussions led to a supplemental project with the US/UK Collaboration on Resiliency and Security (ColoRS) on to the efficacy of RF and acoustic sensors for autonomous applications. This project was completed in Year 7, where a final report was provided to DHS.

**NUSTL**

In addition to NUSTL's engagement in the Center's research projects, the Lab has played a role in the MSC's educational programs. This past year, NUSTL personnel participated in the Summer Research Institute's final presentations session and served as poster judges and panelists at the COE 2021 Summit.

**CBP**

CBP Officers from CBP Field Operations at the Port of NY/Newark provided subject matter expertise for two of the Center's SRI 2021 student research projects. They also participated in the student's final presentation session held virtually on July 8, 2021.

**PANYNJ**

Michael Edgerton, Manager of Port Security for the Port Authority of New York and New Jersey (PANYNJ) has invited the MSC to participate as a member in the agency's new Information Security Exchange program. The program aims to communicate cybersecurity concerns across port partners in the Port of New York/New Jersey. The group has also been in communication with the MSC to discuss opportunities for Maritime Cybersecurity professional development courses.

**DHS COEs**

MSC's director of education served as a co-chair for the COE Summit's education planning committee. In this capacity, she assisted in developing, managing, and coordinating the Summit's student activities to include the poster competition, workforce development panels and the Grand Challenge event. This role also included networking and engagement with homeland security professionals across the DHS enterprise, including DHS S&T, USCG, CBP, US Secret Service, among other DHS components and national laboratories.

## 5.3 Other Activities

In addition to the activities discussed above, MSC conducted many targeted communications efforts.

The Center generated a monthly email newsletter that was distributed to the Center's stakeholders. These updates proved to be an effective way to communicate MSC's activities with its government partners and generate discussions among DHS components on areas of interest.

The monthly update contains relevant information regarding the Center's research, stakeholder engagements and student achievements. An archive of MSC's update newsletters can be found on the Center's website at: https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/center-newsletters.

## 5.4 Management Activities

The main COE management activities not discussed earlier in this report are summarized in this section. The Center Director worked with the COE's Principal Investigators (PIs) to revise project work plans and discussed project content that will benefit DHS and its stakeholders. The Director also worked closely with the DHS Program Manager and spoke with her on a regular basis to understand DHS expectations from the Center and bring up any issues of concern and to adjust operations based on additional OUP COE requirements. Based on these discussions and meetings, the Director held regular meetings with individual PIs as well as coordinated conference call meetings with the Center's PIs as needed. The purpose of these meetings was to ensure that the individual projects are progressing according to the work plans and continue to be aligned with DHS OUP's expectations.

During the COVID-19 pandemic, MSC lead and partner universities closed and restricted all travel activities. To ensure that the projects were minimally impacted, MSC developed a contingency plan that took into account various potential re-opening dates and realigned the schedules to allow research activities to continue without having the need for face-to-face meetings and to change the project end dates. In addition to the contingency plans, the frequency of meetings with PIs was increased to weekly until the various projects were back on track.

Members of the Center Science and Education Advisory Committee (SEAC) have been

engaged periodically throughout the year and were kept informed of the Center activities through phone conversations and Center email communications. In addition, they were invited to Center activities including the Summer Research Institute.

In addition to the above activities, the Center Director continued to reach out to many DHS stakeholders at various levels and in different capacities to discuss their projects and how the Center can be a resource to them. These meetings included discussions with representatives from NUSTL, CBP Air and Marine Office, and various USCG key people. Also, MSC worked closely with the USCG RDC and NUSTL regarding research in the area of counter-UAS systems, such as developing requirements, testing, and quantifying their performance. The Director also discussed transition ideas with CBP Air and Marine Office personnel to understand their needs and their limitations in preparation for transitioning projects when they are ready. In particular, many discussions were focused on current sensors for detecting and tracking underwater and water surface threats.

As part of its transition efforts, the MSC management has continued to conduct project evaluations and tracking of post-project developments. Discussions and meetings were conducted with the Stevens Office of Innovation and Entrepreneurship to discuss potential patents and licensing of research Intellectual Property that is expected to result from the MSC projects.

In addition, MSC management continued to work closely with DHS Intelligence and Analysis Directorate and the National Maritime Security Advisory Committee (NMSAC).

### 5.5 Center Guidelines and Policies

During Year 1, MSC administrators created a document for the Center's academic partners and research PIs containing general orientation information (e.g., partner contact information, reporting requirements, and DHS acknowledgement and disclaimer statements), and copies of the Center's policy and security requirements for handling sensitive material, as well as student safety and security guidelines. The MSC General Information and Guidelines for Academic Partners document was updated in Year 7 and shared with each of the MSC partner schools, with the requirement that they acknowledge receipt and confirm that they have reviewed and understand the policy and security requirements for handling sensitive material and the student safety and security guidelines.

In Year 7, the Center also updated its Student Safety Procedures and Guidelines to include relevant guidance regarding on-campus and field-based internship protocols for use during COVID-19.

## 6 Budget

The budget breakdown is being provided separately as part of the Stevens financial reporting requirements. The accompanying Excel file provides a summary of the funds (actual and budget) per project and per object code (e.g., salary, fringe, travel, overhead, supplies, etc.). Please note that the numbers included are based on numbers available in the financial reporting system at the time this document was prepared. Some expenses

and credits may not have posted when this report was prepared and will consequently be reflected in future financial reporting.

# APPENDIX E-1 SRI 2020 Student Survey

MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Summer Research Institute 2021

2021 - Student Survey

**Your feedback is very important and will help us assess the impact of the SRI on your learning gains and professional development and will help us improve the summer research program for future participants.**

**Please take the time to provide us with as much detailed information as possible in the open-ended questions. <u>All responses are anonymous.</u> Thank you in advance for your time and feedback!**

* 1. How would you describe your knowledge of the maritime domain/enterprise prior to the start of the SRI?

- 1=No prior knowledge
- 2=Minimal knowledge
- 3=Working knowledge
- 4=Advanced knowledge

* 2. Prior to the SRI had you taken any classes online? (via remote learning?)

- Yes
- No

* 3. To what extent has the SRI enhanced or improved your skills in the following areas?

2=Some Improvement from when I 3=Significant improvement from

| | 1=Not at all | | started the SRI | | when I started the SRI |
|---|---|---|---|---|---|
| Ability to Conduct Research | ○ | | ○ | | ○ |
| Communication Skills | ○ | | ○ | | ○ |
| Leadership Skills | ○ | | ○ | | ○ |
| Networking | ○ | | ○ | | ○ |
| Oral Presentations | ○ | | ○ | | ○ |
| Professional Confidence | ○ | | ○ | | ○ |
| Teamwork/Collaboration | ○ | | ○ | | ○ |
| Organizational Skills | ○ | | ○ | | ○ |
| Self-Motivation | ○ | | ○ | | ○ |

Other (please specify)

* 4. Which of the skills above did you improve the most and what SRI activities helped you improve them?

* 5. What skills have you developed or enhanced during the SRI that you feel will be of most use to you in your academic program and future career?

* 6. Rate the SRI in regards to the following items:

| | 1= Not good | 2= Good | 3= Very Good | 4= Excellent |
|---|---|---|---|---|
| Faculty Mentor Guidance and Support | ○ | ○ | ○ | ○ |
| Program Coordination/Administration | ○ | ○ | ○ | ○ |
| Program Format | ○ | ○ | ○ | ○ |
| Guest Speakers | ○ | ○ | ○ | ○ |
| Teamwork/Collaboration | ○ | ○ | ○ | ○ |
| Stakeholder Engagement in Projects | ○ | ○ | ○ | ○ |
| Research Project Outcomes | ○ | ○ | ○ | ○ |
| Use of Slack | ○ | ○ | ○ | ○ |
| Weekly Status Update Meetings | ○ | ○ | ○ | ○ |
| Student Projects (How did you feel about the project you were assigned?) | ○ | ○ | ○ | ○ |
| Student Team Dynamics. (Did the members of your team collaborate and contribute equally to your research project?) | ○ | ○ | ○ | ○ |

* 7. How would you best describe your experience in the SRI and what are your top takeaways from the program?

* 8. What would you say are the strengths of the SRI?

* 9. What would you say are the program weaknesses and what can the MSC do to improve the program if it is held remotely again next summer?

* 10. Has the SRI enhanced your interest in pursuing a career and/or further academic study in the field of maritime/homeland security?

Yes

No

* 11. Would you recommend the SRI to your friends and colleagues at your university/school?

Yes

No

# APPENDIX E-2 Maritime Transportation Cybersecurity MSI Workshop Survey

MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Cybersecurity in the Maritime Transportation System (MTS) and other Critical Infrastructure Workshop

Workshop Feedback Form

**Dear Colleague,**

**The Maritime Security Center would like to request your feedback on your recent participation in the Center's Cybersecurity in the MTS Workshop. Your feedback is important to us and will help shape and guide how we deliver the program in the future. We appreciate your constructive comments and thank you for your time.**

* 1. What best describes you?

- ○ Higher Education (College-level) Faculty Member
- ○ Higher Education Administrator
- ○ DHS / USCG Professional
- ○ Other (please specify)

* 2. What inspired you to attend the Workshop? (Check all that apply.)

| Did not meet my expectations. | Met my expectations. | Exceeded my expectations. |
|---|---|---|
| ○ | ○ | ○ |

Other (please specify)

- [ ] The topic is relevant to my job/academic program.
- [ ] I was hoping to learn new information that will assist me in my classroom.
- [ ] I am looking for new curriculum materials to include in my classes.
- [ ] I am interested in creating a new program in Maritime Cybersecurity.
- [ ] This was an opportunity to network with fellow colleagues.
- [ ] Other (please specify)

* 3. Did the Workshop content meet your expectations?

* 4. What aspects of the Workshop were of most interest and relevance to you? (check all that apply.)

- [ ] USCG Perspectives on Maritime Cyber and the MTS.
- [ ] Introduction to the Maritime Transportation System.
- [ ] Discussion on IT and OT Systems and Vulnerabilities.
- [ ] Other (please specify)

* 5. Rate the Workshop in regards to the following items:

| | Not good at all | Good | Very Good | Excellent |
|---|---|---|---|---|
| Quality of the Workshop Curriculum | ○ | ○ | ○ | ○ |
| Quality of Instruction | ○ | ○ | ○ | ○ |
| Quality of Workshop Coordination/Administration | ○ | ○ | ○ | ○ |
| Ease of the Online Platform (Webex) | ○ | ○ | ○ | ○ |
| Participant Engagement and Dialogue | ○ | ○ | ○ | ○ |

* 6. Prior to attending the Workshop, had you discussed or incorporated examples of maritime cybersecurity concerns in your curriculum plans or programs of study?

- [ ] Yes
- [ ] I have not up until this point, but I will now consider incorporating discussion into my curriculum.
- [ ] No and I am unlikely to include mention or examples of this in my curriculum.
- [ ] Not applicable
- [ ] Other (please specify)

* 7. What were your top takeaways from the Workshop? (Check all that apply.)

- [ ] Curriculum discussion
- [ ] Discussions and networking
- [ ] Inclusion of the U.S. Coast Guard
- [ ] Other (please specify)

8. What can the Maritime Security Center do to improve the Workshop for future participants? (Please provide as much detail as possible.)

9. Would you be interested in collaborating with the MSC/Stevens Institute of Technology to host future workshops or engage in collaborative research projects?

- [ ] Yes
- [ ] Not at this time, but maybe in the future
- [ ] No
- [ ] If yes, please let us know how you would like to collaborate.:

10. Additional feedback/comments regarding your experience in the Workshop. (optional)