MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

The Maritime Security Center (MSC)

at Stevens Institute of Technology

Hoboken, NJ

Annual Report

Year 3

July 1, 2016 through June 30, 2017

Submitted on August 31, 2017

APPROVED November 14, 2017

TABLE OF CONTENTS

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 3 (July 1, 2016 through June 30, 2017).

MSC is composed of a consortium of internationally recognized research universities, including Stevens, MIT, the University of Miami, the University of Puerto Rico, Louisiana State University, Florida Atlantic 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 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, 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 Satellite Surveillance, Port Resiliency, Maritime Cybersecurity, and VTS Radar research projects. These projects were in the work plan that was approved for Year 3.

2.1. Satellite Surveillance

2.1.1. Introduction

Open ocean satellite-based surveillance is a key capability in the development of Maritime Domain Awareness (MDA), particularly with respect to ship detection, classification and identification. While large vessels are required to carry Automatic Identification System (AIS) transponders, smaller vessels, in particular, go-fast, semi-submersibles and other small boats do not transmit a similar message providing basic information of ownership, ship characteristics, position, speed and course, and destination. These vessels are often used as a means to transport illegal drugs and contrabands as well as smuggling and trafficking of humans and pose a severe threat to our national security. They operate in the coastal domain but outside the range of terrestrial radar stations and move at low light

conditions to elude detections by law enforcement ships and aircrafts. However, satellite synthetic aperture radars (SARs) are sensitive to roughness modulations of the ocean surface and motions of fast moving targets. SARs have demonstrated to readily be able to detect vessels of medium to large lengths. New satellite systems have improved imaging modes and spatial resolutions to allow detections of even smaller boats and non-emitting targets. New algorithms to detect wakes of boats can now be used to detect the presence of small, non-emitting boats.

2.1.2. Project Objectives

The purpose of this phase of the project (Phase II) is to build on the Phase I work where satellite data and products were tested for integration into the Air and Marine Operations Surveillance System (AMOSS), operating at the Air & Marine Operations Center (AMOC) utilizing specific formats. Phase I included testing of a delivery path that provided timely and actionable information to the AMOC.

Phase II work demonstrated the ability of the Center for Southeastern Tropical Advanced Remote Sensing (CSTARS) facility at the University of Miami to provide open ocean satellite-based surveillance information to the AMOC in Riverside, CA. In particular, it demonstrated the ability to receive tasking from the AMOC to detect vessels and provide relevant and timely data to improve Maritime Domain Awareness and enable the tactical operations of DHS Components.

The Phase II Workplan was approved on March 30, 2016 and work began on April 5, 2016. This report provides the work accomplished since the start of the project to the end of the Project. Table 1 lists the Critical Operations needed to be achieved in sequence to realize the ultimate goal of Phase II - to provide open ocean satellite-based surveillance information of detected vessels to the Air and Marine Operations Center and provide relevant and timely data to improve Maritime Domain Awareness and enable the tactical operations of DHS Components. Weekly teleconferencing involving AMOC, DHS S&T, MSC, and CSTARS personnel to review current progress, discuss issues, and plan for future goals were conducted.

2.1.3. Research Milestones Met

Measures of effectiveness (MOE) that have quantitative and/or qualitative evaluation criteria are rated “Pass” or “Fail.” Those areas that do not have evaluation criteria, but where information is needed for the decision-maker are reported using narrative format. Aggregation of the results are used to determine how well each MOE is achieved, and in-turn, the MOEs was used to resolve the Critical Operational Issues (COI). The test team (*i.e.* AMOC) will use all results, combined with test team operational experience and mission expertise, to answer each COI. The objectives chosen for this experiment should determine the law-enforcement operational utility of CSTARS to contribute to the maritime wide area surveillance requirements of DHS and AMOC. This experiment should also determine if CSTARS can reliably detect “dark targets”. Phase II exploratory effort would perform the following Critical Operations (CO) listed below.

Table 1: Critical Operation for Phase II

Critical Operations (CO)	Milestone: Phase II	Performance Metrics	Status
CO-1	CSTARS will establish connectivity with AMOC Operations and display pertinent track data in the AMOSS. This connectivity will be tested using archived test data for cost savings purposes. AMOC will assist with the connectivity as needed.	Establish different connectivity links (open & secure) to evaluate reliability and robustness. **Testing parameter will be data rate and transmission time of various file sizes at different times of day.**	Transfers performed well. VPN password expires and must be reset. AMRDEC transfers work well for imagery, but is very cumbersome.
CO-2	CSTARS will transmit satellite test data to display in AMOSS, as well as Satellite Automatic Identification System (S-AIS) data that shows tactical locations of all vessels in the immediate area of the target vessel.	Perform data transmission tests with S-AIS data to evaluate reliability and robustness. **Testing parameter will be data rate and transmission time of various file sizes at different times of day.**	Transfers performed well. VPN password expires and must be reset.
CO-3	CSTARS test data will be formatted for display in AMOSS and show detected targets details such as: a. Synthetic Aperture Radar (SAR) target b. target position c. target course d. target speed e. Provide some parameters on Probability of Detection (PD) and Probability of False Positive (PFP) for various classes of maritime vessels.	Test data will be reproduced at data formats consistent for display in AMOSS. This testing will involve the detection and location of targets in exploitable data sets for display in AMOSS. The detection reports received by AMOC will include PD and PFP for various vessel classes. **Detection in a) will be compared to S-AIS based data in b) to c). Test parameter e) will be computed from known data sources (e.g., S-AIS and T-AIS data).**	SAR target detections and positions readily available. Target speed (d) not yet able to be established from imagery. Target heading can be established with 180 degree ambiguity.
CO-4	After completion of CO-1 through CO-3, CSTARS will conduct a live data test with AMOC, delivering CO-1 through CO-3 in near real time.	Establish timelines of the TCPED (Tasking, Collection, Processing, Exploitation, and Dissemination) process. **Testing parameter will be time to deliver actionable**	Live test of collection, processing and dissemination of SAR detection product was performed satisfactorily.

		and exploitable data products to AMOC in live test.	
CO-5	After successful completion of CO-4, CSTARS will conduct four follow-on tests to demonstrate time latency for real time tasking using SAR and EO imagery as follows: a. pre-arranged between CSTARS and AMOC in ScanSAR Narrow and ScanSAR Wide mode at specific dates and times to demonstrate time latency of tasking and ensure that the data can be displayed in a tactical environment. b. Upon successful completion of the scheduled tests (a), two no-notice tests will be completed using ScanSAR Narrow and ScanSAR Wide mode during normal working hours Monday-Friday between the hours of 0900-1700 Eastern Time. c. Focus areas of tests will be the East Pacific AOR out to 200 NM, the Florida Straits, or the Gulf of Mexico. Specific locations to be imaged will be identified by the AMOC.	Establish timelines of the TCPED process in a tactical actionable timeframe for different satellite imagery data (i.e., modes) under different conditions and settings as well as locations. **Testing parameter will be time latency to deliver actionable and exploitable data products to AMOC and data product quality for display to AMOSS in tactical environment.**	Unable to perform satisfactorily due to lack of additional financial resources. A single test was performed, but was not useful to establish any meaningful metrics.

Expected outcome of ***Phase II: Operational TCPED Capabilities*** to provide CSTARS' multi-sensor satellite data and products to AMOSS. The completion of Phase II testing of satellite data and products for enhancing the operational picture of the maritime domain will include an E2E "live" test in near-real time for a simulated response by AMOC.

Initial discussions focused on data formats suitable for ingestion into the AMOSS system. AMOSS decided upon raw satellite AIS (S-AIS) National Marine Electronics Association

(NMEA) format. For radar imagery information, the OTH-GOLD format with image chips from detected vessels. CSTARS provided samples of both formats for ingestion into the AMOSS system.

The electronic transfer of data was the next subject addressed. CSTARS provided AMOSS a network connectivity capability as per the AMOC's request. The electronic transfer method selected was secure File Transfer Protocol (sFTP) over a Virtual Private Network (VPN) with CSTARS pushing data across the network and AMOC automating a system to transfer data to their servers. AMOSS established a VPN connection and CSTARS tested the connection. First tests were with manual data transfers, then with automated transfers via a python script. A small data set of S-AIS and OTH-GOLD data were repeatedly transferred across the network for 15 days. 1758 files (about 38 GBs of data) were transferred at an average transfer speed of 1100 kbits/sec. This was deemed as acceptable by the AMOC.

COI-1/2

Electronic connectivity between the CSTARS and the AMOC was developed in two different streams intended for different AMOC entities. One stream is for small file products such OTH-GOLD (COI-1) and S-AIS NMEA (COI-2) data and direct ingest into the AMOSS. The second data stream is intended for the Production, Exploitation, Dissemination (PED) cell and manual imagery exploitation. COI-1 and COI-2 are discussed together since the transfers of both file types (OTH-GOLD and S-AIS) are each textual file types intended for AMOSS and would be transferred as a unit under operational situations. Each stream type is discussed below.

For the small file data steam to AMOOS, a virtual private network (VPN) was established. Files were pushed over the VPN using secure File Transfer Protocol (sFTP). CSTARS developed a python script to connect to AMOC VPN, transfer files with sFTP, and disconnect from the VPN. CSTARS archived data was used to produce 11 test data sets (OTH-GOLD, target image chips, and S-AIS NMEA) ranging from around 3 MBs to 24 MB in size. From this data set, a group of files (from 1 to 11) was randomly selected and transferred to the AMOC. The quantity of data and the time required for transfer was recorded. The process of random data selection, VPN connection and file transfer was repeated on an hourly basis. Initial testing failed to an expired VPN password. With the password reset, the testing resumed from 5 July to 20 July 2016. During this time, 1758 files (around 34 GBs) were transferred. The average transfer rate was 1100 kb/sec (and 63 kb/sec standard deviation). This was deemed within the expected data transfer rate. See Figure 1 below.

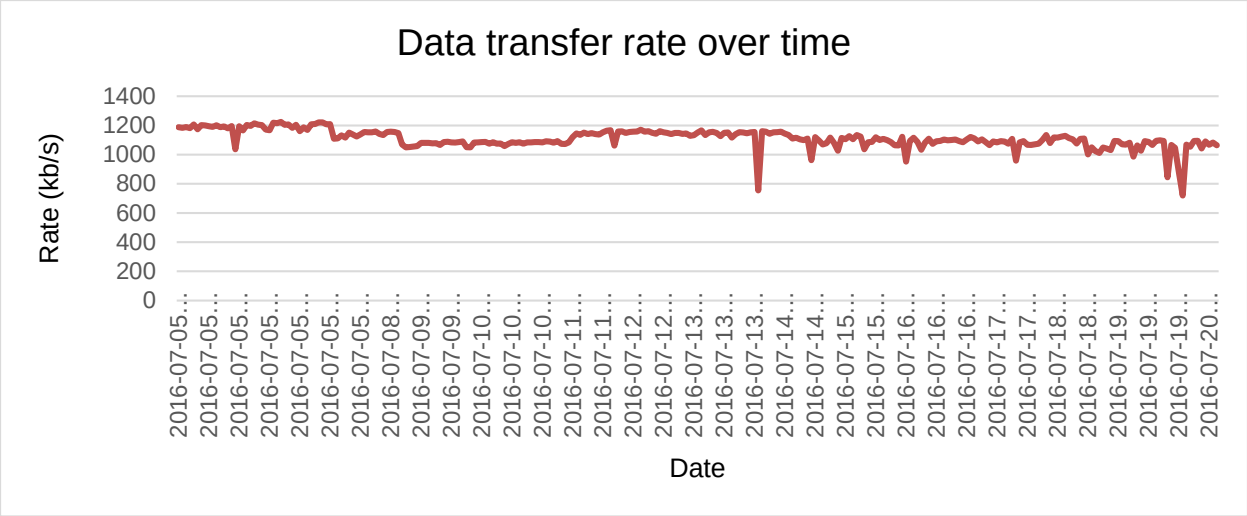


Figure 1: Summary of small file data transfer rates.

Data rates were also examined at different times of the day. Average test speeds appeared stable through the day. See Figure 2.

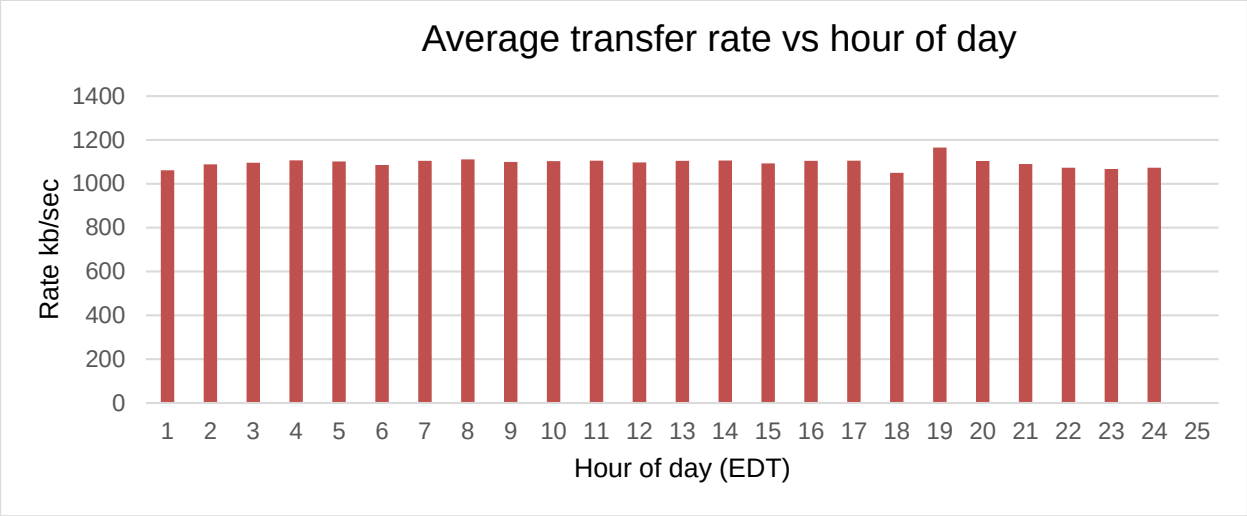


Figure 2: Summary of small file data transfer rates vs time of day.

Although the VPN/sFTP method was not intended for the transfer of large files (i.e., full image scenes), this scenario was tested. Full image files are not intended for AMOSS. Thirteen full image files with data sizes in the range of 210 MB to 642 MB were selected. The testing preceded much like the small file data set with the exception that for any transfer event only a single image file was randomly selected (as opposed to the possibility of transferring multiple small files in a transfer event). Testing occurred from July 26

to August 11, 2016 and a total of 58 files (28 GBs of data) were transferred. See Figure 3.

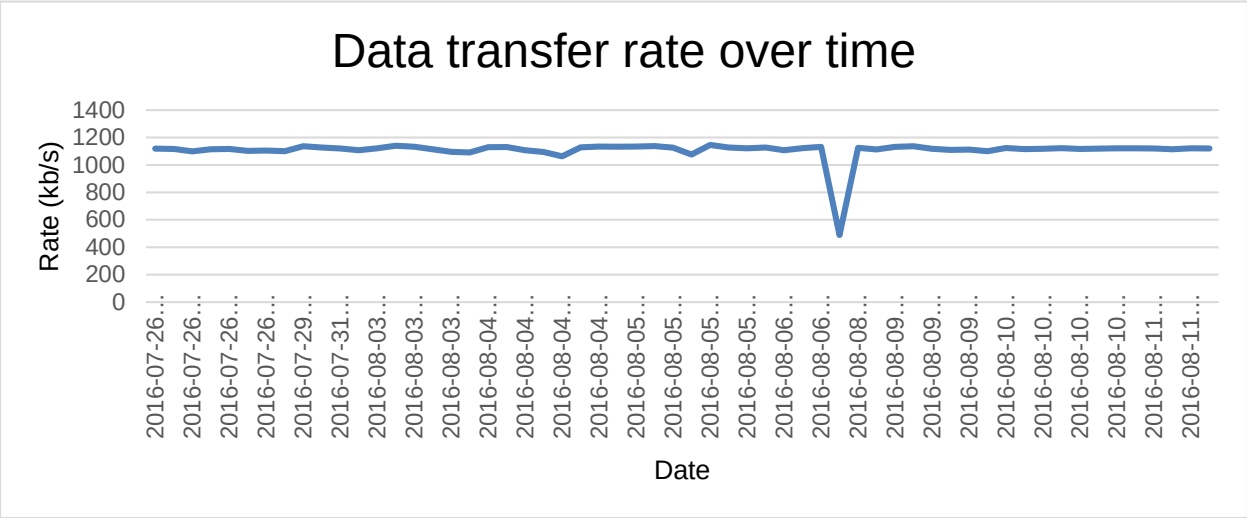


Figure 3: Summary of large file data transfer rates.

There does appear to be a drop in the file transfer rate between 2016-08-08 09:04:30 and 2016-08-08 11:46:22 EDT. The reason for the drop in the transfer speed is not known.

The second data stream is intended for the PED and technically not part of the Statement of Work (SOW). However, since the PED is interested in the full image scenes for exploitation it is natural to transfer this data as well. Rather than full image data files examined by the PED, files were transferred via US Army AMRDEC Safe Access File Exchange (SAFE). While this provided a path to get imagery data to the PED cell, this is an operationally viable method to do so. Another transfer for imagery needs to be established. No time metrics were established for the AMRDEC transfers. In summary, the full capability level can be attributed to the VPN/sFTP connection which provided secure and reliable data transfers to AMOSS.

COI-3

The data format for targets derived from SAR is OTH-GOLD text file with accompanying target image chip(s). The data format for S-AIS is the National Marine Electronics Association (NMEA) 0183 format.

The OTH-GOLD format ingest into AMOSS was verified on 27 September 2016 during the CSTARS site visit to the AMOC. The target chips cannot be ingested in the AMOSS system and were not used (see example in Figure 4). Currently, target speed cannot be estimated solely from SAR imagery. However, correlation with AIS may help with target speed estimation. Target heading can sometimes be established with a 180 degree ambiguity, especially in open ocean conditions.

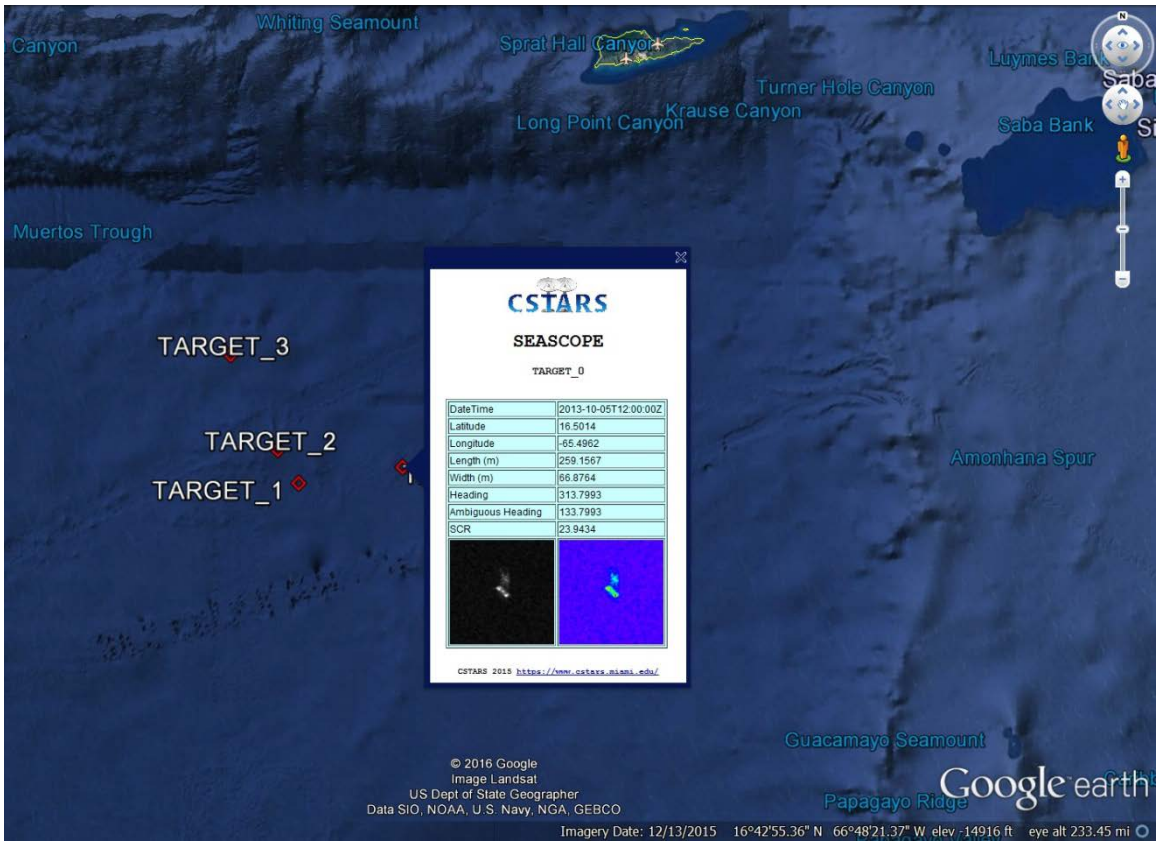


Figure 4: Image chip associated with a detected target in a SAR image which is a routine output product generated by CSTARS' SeaScope.

The S-AIS ingestion into AMOSS was not tested but due the standardized nature of the NMEA data format, it is expected to be easily ingestible by the AMOSS. For the full scene image data, the SIDD/GEOTIFF was determined acceptable for the PED cell. In summary, the full capability level can be attributed to CSTARS' OTH-GOLD format that was readily ingested into the AMOSS.

Analysis: S-AIS and SAR satellites as they exist today are in different orbital planes (and will very likely change in the next few years). This means that S-AIS detection and SAR imagery detection cannot occur simultaneously in the AMOC area of responsibility (AOR). In order to correlate AIS and SAR information, AIS data must be projected over a period of several hours. Given that an image position and time are known, AIS data before image collection in the general vicinity of the target can be analyzed and projected to give an estimated vessel position at imaging time and an error ellipse/cone/polygon showing the uncertainly of a vessel's position given its recent S-AIS vessel course and speed. This error ellipse would greatly aid the possibility of correlating S-AIS with SAR detected targets. However, it is unknown at this time if the AMOSS can support ellipse/cone/polygon data types (see example in Figure 5).

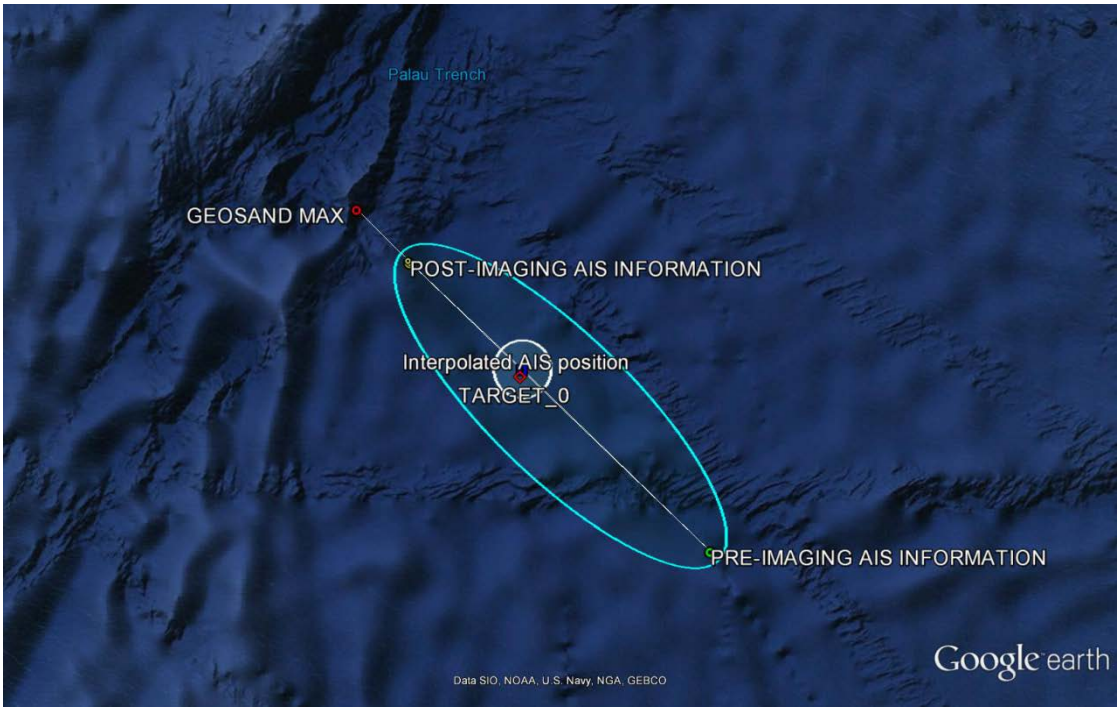


Figure 5: Uncertainty ellipse associated with a detected target in a SAR image which is a routine output product generated by CSTARS' SeaSentinel.

COI-4

The live test was conducted during the CSTARS site visit to the AMOC on September 27, 2016. Two Areas of Interests (AOIs) where described by Mr. Curtis Brown and CSTARS generated kml files based on this description. The following two AOIs are shown Figures 6 and 7.

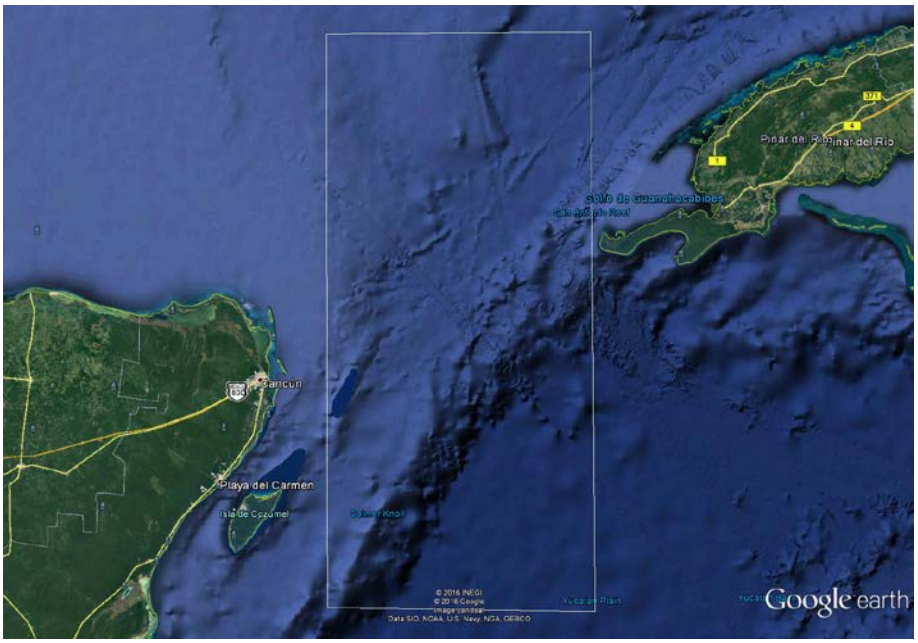


Figure 6: Yucatan/Cuba AOI

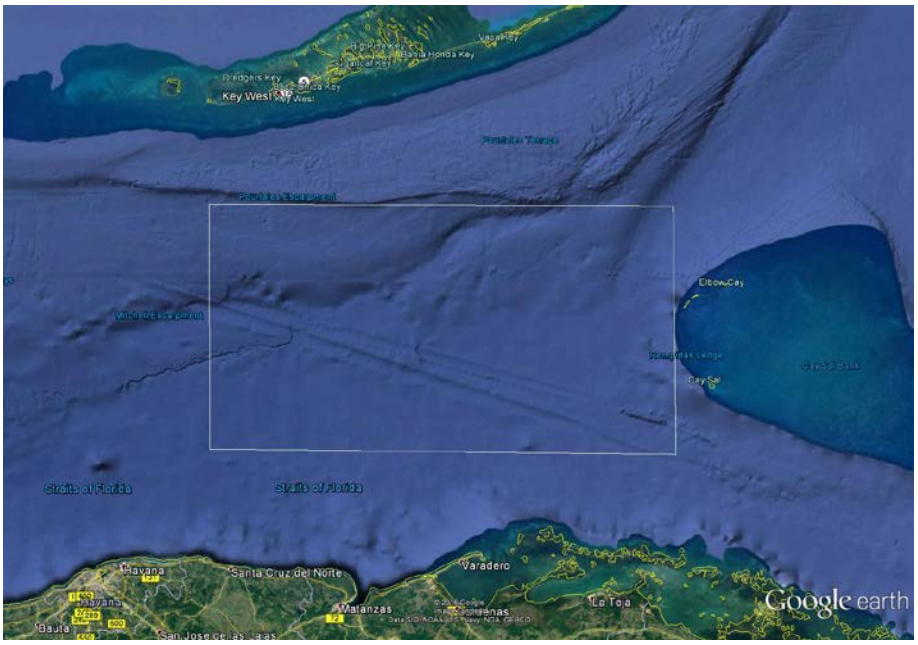


Figure 7: Florida Straits AOI

In order to maximize the probability of detecting targets, the MarineTraffic website (http://www.marinetraffic.com/) was examined. MarineTraffic collects and displays AIS data. It also provides 'heatmaps', areas of greatest AIS density. These AIS heatmaps were consulted to locate the areas of greatest AIS density within the provided AOIs. The

image test areas were selected upon the union of these two inputs. See Figures 8 and 9.

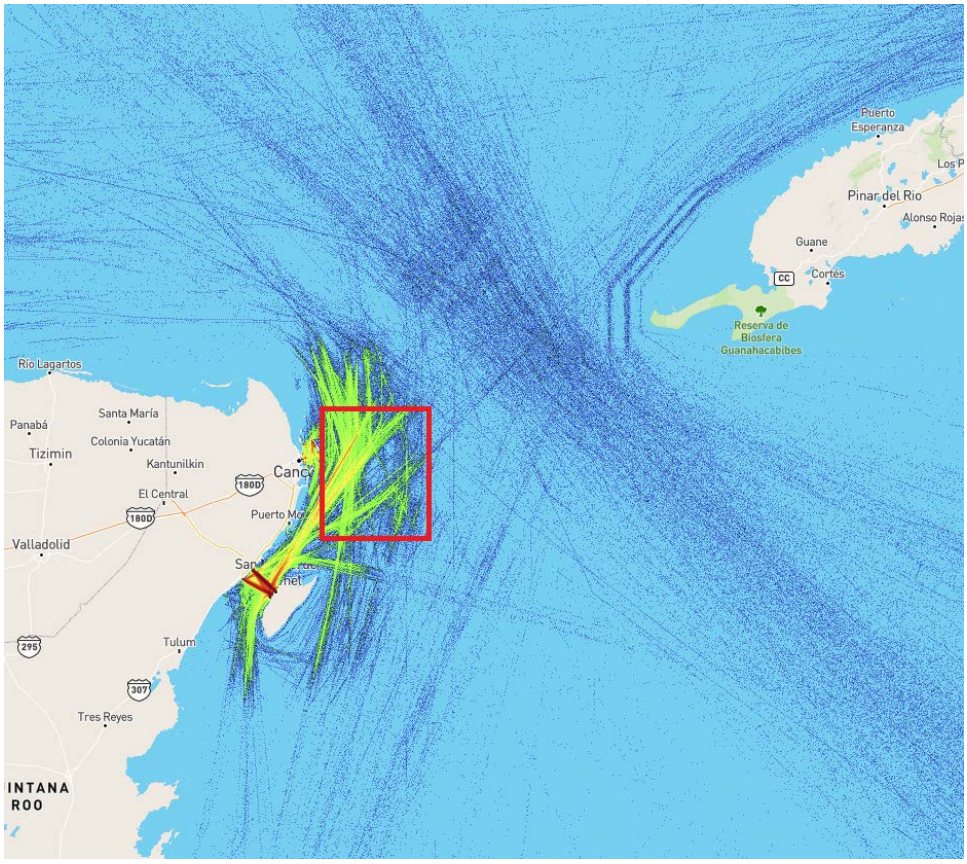


Figure 8: MarineTraffic heatmap in Yucatan/Cuba AOI with red box showing approximate imaging area.

The Yucatan/Cuba AOI SAR image was collected on September 27, 2016 at 11:52:00 UTC. The SAR satellite used was Cosmo-SkyMed-1 with Horizontal Transmit/Horizontal Receive (HH) polarization and stripmap beam mode H4-24 (incidence angle 51.5º-51.98º). CSTARS' SeaSentinel software was executed on the collected image with a very low threshold setting. This increases the chances of detecting targets but also increases the chances of false alarm. This was done in order to increase the probability of some detected output, even with false alarms. This was indeed the case of the collection on September 27, 2016, with the detected targets deemed to be false alarms. However, this

data set still provided the opportunity to test the ingestion of OTH-GOLD data in the AMOSS which was successfully accomplished.

The Florida Straits collection remains unfulfilled.

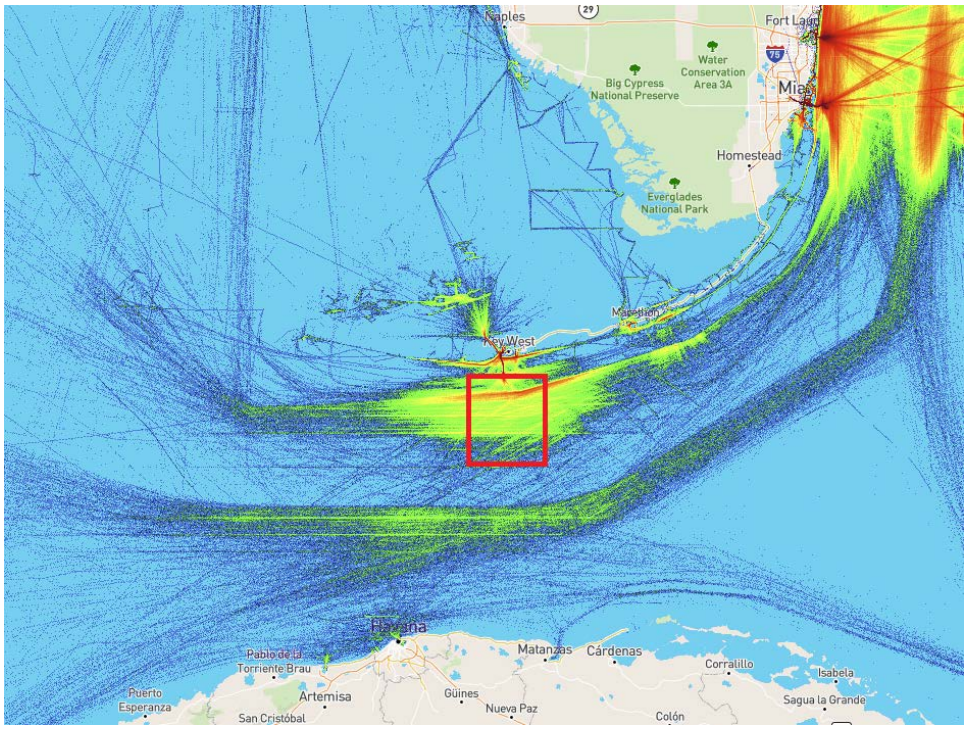


Figure 9: MarineTraffic heatmap in Florida Strait AOI with red box showing approximate imaging area.

In summary, the full capability level can be attributed to CSTARS' OTH-GOLD format which was readily ingested into the AMOSS without modification.

COI-5

COI-5 was not completed due to the available funding levels and therefore was not attempted. The primary reason was that one single satellite collect would allow for deriving any meaningful metrics and/or statistics. For example, if the collect and execution would be successful, this would imply a 100% success. On the other hand, if the collect would have failed or some task would not have been timely, the result would have been a failure. In summary, both outcomes would have been meaningless since the first one would not guarantee future successful results and the latter one would not have allowed to determine the failure and trace the process where the failure occurred.

In addition, the following was accomplished:

a. Visit AMOC, at March AFB in Riverside, CA on September 26 and 27, 2016

The PI and Dr. Paul Mallas visited AMOC to be on site while testing data transfers and resolve format issues as well as plan ahead for live testing. Other topics relevant to the project were also discussed.

b. Weekly Telcon to discuss progress and future work continuing on July 5, 2016

Telcons involved CSTARS, AMOC, MSC, and DHS personnel to focus specifically on COs progress and mitigate any potential problems with future Critical Operations were conducted. The weekly telcons were suspended after October 26, 2016.

c. Telcons at specific dates to discuss DHS S&T SAR / EO Pluglet

CSTARS participated to support DHS personnel preparing and executing the SAR / EO Pluglet. CSTARS also participated in the Pluglet as a User to demonstrate its capabilities of detecting small vessels.

d. Homeland Security Open Source Tactical Geospatial Intelligence Plugfest meeting on February 13 to 16, 2017

P. Mallas attended the meeting by Homeland Security on Open Tactical Geospatial Intelligence Plugfest presenting the results obtained during the ship detection exercise for small vessels.

2.1.4. Conclusions

CSTARS has shown the ability to provide Maritime Domain Awareness data to the AMOC in simulated and near-real time tests. Data including OTH-GOLD targets derived from SAR imaging satellites, S-AIS NMEA data, and full scene images have all been provided. And for a single test case, this data has been provided in near real time. Data transfer occurred at consistent speed within the expected data transfer rates. File formats were ingested into the AMOSS successfully and full image scenes were ingested and exploited in the PED cell. Single near-real time test occurred successfully and a remaining collection still being planned. A single COI could not be completed due to lack of funding to execute it. However, the other four COIs were successfully completed with minimal challenges.

2.2. Port Resiliency

2.2.1. Introduction

Led by Florida Atlantic University and including collaborators from Louisiana State University (LSU) and University of New Orleans (UNO) this project is aimed at developing a modular, simulation based, tool to assess and plan for resiliency of a port to major natural and man-made disruptions. Resiliency of a port is defined in terms of the severity of the impact of the disruption to a performance measure such as port capacity and

throughput as well as in terms of the duration of the impact on the performance measure. Micro and mesoscale modeling and simulations of port operations enable quantifying the consequences of a disruption at a port and associated responses in support of avoidance and mitigation of damage and capacity reduction, and aiding rapid recovery from disruptions. The project involves development of a simulation model for selective intermodal facilities that covers operation and logistics and study and analysis of optimization problems related to resilience that are commonly encountered in intermodal/port facilities to incorporate various stochastic elements such as uncertainty for the terminal's performance measures in order to evaluate the performance of optimization algorithms under different scenarios. The research and the tool being developed will provide better understanding of the consequences of disruptions at a port.

The Year 3 effort involved completion of modeling and simulation tasks, and engagement of stakeholders.

2.2.2. Project Objective

The principal objective is to develop a cost-effective port resiliency assessment and planning tool that can be adapted, through a choice of interchangeable event modules, to assess and plan for evolving threats and hazards to a port and its waterside and landside distribution capacity, in support of avoidance and mitigation of damage and capacity reduction, and aiding rapid recovery from disruptions. The aim is to develop an integrated tool based on a systems approach to port distribution capacity, port operations, risk management, and policy and jurisdiction considerations and involving simulation and modeling.

Other objectives include: 1) Development of a simulation model for selective intermodal facilities that is going to cover operation and logistics, 2) Study and analysis of optimization problems related to resilience that are commonly encountered in intermodal/port facilities to incorporate various stochastic elements such as uncertainty for the terminal's performance measures in order to evaluate the performance of optimization algorithms under different scenarios, and 3) Promotion of graduate and undergraduate education in transportation and marine engineering.

2.2.3. Research Approach and Tasks

The tool development is based on modeling and simulation, taking a systems approach to port distribution capacity, port operations, risk management, and policy and jurisdiction considerations. Risk management of a catastrophic event (Conger, 2011) involves careful assessment of the vulnerability of the port to natural and human-caused catastrophic events; implementation of prevention or risk reduction measures to avoid or mitigate damage; advance preparation for quick and effective response and proactive measures to ensure financing is available to cover the costs of response and recovery. Principal considerations in the approach include:

- *Identification of threats and hazards to port transportation system*

- *Safety, security and resiliency of the port infrastructure*: Requirements for port operations and increase in capacity, weather readiness, exposure and mitigation of threats and hazards, disaster response
- *Safety, security and resiliency of the waterside distribution capacity*: Requirements for sea freight, navigation infrastructure, ship traffic management, maritime surveillance, weather readiness, exposure and mitigation of threats and hazards, disaster response
- *Safety, security and resiliency of the landside distribution capacity*: Requirements for road and rail freight, road and rail infrastructure, Intermodal connections, weather readiness, exposure and mitigation of threats and hazards, disaster response
- *Interagency and stakeholder coordination*: Community resources and societal impact, compliance with policy, jurisdiction and maritime security governance

The basis of the simulation is the integrated modeling software Aimsun NG (Xiao et el., 2005), which is used in transportation simulations by governments, planners, industry and academia worldwide.

Identified Tasks

The tasks for Year 3 were Tasks 11 through 13. Tasks 1 through 12 are the scope of Years 1 and 2 and are listed for reference. Task 11 is completed, Task 12 is modified to focus on lessons learned as requested and Task 13 is now due for completion by 10/31/2017.

Task 1a. *Develop detailed work plan*

Task 1b. *Define the port system and scope of the project*

Task 2a. *Assess port vulnerabilities*

Task 2b. *Identify characteristics of external disruptors*

Task 3. *Establish port rules, policies and decision-making process*

Task 4. *Define requirements for the tool*

Task 5. *Develop strategies for the development of the tool*

Task 6. *Develop simulation model and conduct initial test and performance validation*

Task 7. *Formulate mathematical model*

Task 8. *Develop optimization models for resiliency and emergency management*

Task 9. *Test and validate mathematical models and optimization algorithms*

Task 10. *Identify and develop a theoretical and empirical basis*

Task 11. Complete modular algorithms and user interfaces for the new tool**.**

Task 12. Engage stakeholders in demonstrations of the tool and evaluate the tool using available real data, basing the evaluation on meeting the requirements established in Task 4.

Task 13. Prepare final report**.**

2.2.4. Research Milestones Met

Research Milestones - Status

Milestone	Performance Metrics	Status
1. Completion of simulation modeling, detailed algorithms and user interfaces for the new port resiliency assessment and planning tool.	The new tool-based predictions of the impact and recovery of port capacity validated against available historical data from 2 to 3 ports involving closure of a port over a period of time ranging from a few days to several weeks.	90% completed. Incorporation of additional data and tool validation underway, to be completed by 10/31/2017.
2. Completion of the development of best practices guidelines and Port Resilience Indices for specific disruptions using the new tool.	The merits of the Port Resiliency Indices and best practice guidelines evaluated through stakeholder feedback. Response from over 30 stakeholders will be sought.	85% completed. Analysis of results is in progress. Task completion by 10/31/2017.
3. Completion of a final report.	Acceptance/dissemination of the report, publication of results in a technical journal and one Transportation Research Board conference, and delivery of algorithms, surveys and related materials to DHS.	In progress. Task completion by 10/31/2017.

2.2.5. Accomplishments

Based on available information and stakeholder discussions, the scope of the project has been defined to include three disruptive scenarios: 1) disruption at Port Everglades due to a major storm, 2) disruption at Port of New Orleans due to an accident involving major oil spill, and 3) disruption at Ports of LA/Long Beach due to a labor dispute. Significant amount of the required data, including AIS data for ship traffic, have been obtained for Port Everglades, Ports of New Orleans, and Ports of LA/Long Beach in support of developing the port resiliency assessment and planning tool. Stakeholder survey

questions have been prepared and Port Authorities and related stakeholders have been contacted. A brief was provided to AMSC in Dania Beach, Florida in August 2016, and a stakeholder workshop on port resiliency was held at FAU in December, 2016 to solicit community feedback.

Literature reviews have been conducted to identify existing related tools, identify threats and associated vulnerabilities, as well as take into account various strategies employed to mitigate impact and to recover from disruptions (See Appendices R-1). The basic elements of the required port simulations on the Aimsun platform have been completed. We are now in the process of incorporating models for linking the waterside and the landside capacities, and stakeholder inputs on responses to disruptions into the simulation to complete the tool. Detailed modeling and integration of Monte Carlo optimization simulation of vessel activities within Aimsun for Port Everglades have been accomplished. The Monte Carlo optimization simulations will provide measures of effectiveness of port operations and landside and waterside traffic under various conditions. They can be used to quantify consequences of a disruption at a port for different levels of threat and for various levels of port resiliency, including length of disruption, loss of capacity and throughput and recovery times. AIMSUN based landside simulation setups have been completed for Port Everglades, Port of New Orleans and Ports of LA/Long Beach. Development of models linking the waterside and landside capacities are underway. Case studies of the various types of disruptions, such as storm-related flooding at Port Everglades, and their impacts have been conducted in support of establishing the necessary databases and conducting validation of the tool.

Stakeholder Engagement

The following stakeholders are identified: Port Authorities (Directors, Captains of the Port, Port operators); USCG; CBP; Army Corps of Engineers; Law enforcement agencies; Port Recovery officers; Port Security Specialists; Port tenants; Railways/Rail companies that transport cargo; Dept. of Transportation (MARAD); NOAA; MPOs; FEMA; Local Communities; and Academia.

A brief on the project was provided to the Sector Miami Area Maritime Security Committee (AMSC) in August 2016. The participants, including local port representatives, USCG, MARAD, and CBP showed significant interest in the project and offered perspectives on how the study would benefit various aspects of port activities.

A successful stakeholder engagement workshop on port resiliency was held at FAU in December 2016 with 45 people in attendance. The objectives of the workshop were: 1) To develop in-depth knowledge and understanding among participants of the issues in port resiliency; 2) To acquire and share information on current and developing efforts in port resiliency and risk management studies; 3) To provide a forum for discussion and feedback on port resiliency tools being developed at FAU; 4) To connect with stakeholders and provide a forum for discussion of future goals for port security and resiliency. Participants included representatives from the USCG, the US Army Corps, Port Everglades, Port of Palm Beach, MARAD, various local and national agencies, and academia. Port recovery and security officers present provided useful input on past experiences with port disruptions, available risk assessment tools, and issues to consider in

developing the tool. The workshop included two breakout sessions: 1) Critical Issues in Assessment and Planning for Port Resiliency and 2) Needs and strategies for enhancing port resiliency. Different ways to assess and quantify resilience were discussed, including the need for post-disaster recovery plans at ports and in neighboring communities. One of the challenges discussed was to find ways of standardizing communications processes within and across ports. ICS was also discussed in this context. With regard to the strategies to enhance resilience, there was agreement among participants that decision-support tools would be helpful and that better tools and technology for assessing port resilience were needed. A better understanding of port governance issues was also discussed as a means to improve port resiliency. In terms of the challenges, there was a discussion about participation by industry partners and leaseholders. Some of that discussion surrounded the kinds of incentives that were needed to spur industry partners to adopt resilience measures, including business continuity plans that aligned with centralized port recovery plans. There was also a discussion about finding standardized solutions and mitigation strategies that would work across all ports. Other issues discussed were the role of insurance and reinsurance and the types of incentives that would work best to enhance port resiliency.

Further, discussions were held with Port Everglades and USCG Sector Miami on application of the tool to address specific issues pertinent to contingency planning, and decision-making leading up to and following a storm-related disruption at the port. Conference call meetings were held with USCG RDC and Sector Miami seeking guidance on transitioning the port resiliency tool to stakeholders.

Stakeholder Surveys

An Institutional Review Board (IRB) approved stakeholder survey questionnaire was developed and was used to survey participants at the December 2016 port resiliency workshop at FAU. The questionnaire deals with the following topics: identification of hazards; hazard assessment; effectiveness of plans and tools; the ability to locate critical infrastructure facilities; internal and external communication and coordination; identification of mutual aid agreements; assessment of coordination and decision-making; continuity of operations planning; understanding of risk management, resources, and insurance; and emergency operations during and post-disruption.

The respondents to the survey fell within three groups/organizations: Ports; U.S. Government Agencies (such as the U.S. Coast Guard, U.S. Army Corp of Engineers, MARAD); Academia; and Third-Party Stakeholders. Overall, the responses to the survey point out several places where there are preparedness measures that have been adopted and what measures have worked. The survey results also show however, that more training in emergency management preparedness is needed and that more buy-in is needed from port employees on why these plans are necessary and important for each employee. To some extent, the survey results show that the Coast Guard could pay more attention to flood management and storm surge management at ports; given the effects of Hurricane Mathew in 2016 and other storms in the future, these factors may be of increasing importance. The results also indicate that more information-sharing and preparedness by tenants, third-party stakeholders, and ports could be helpful.

While increasing coordination and building resilience was valued, the comments from the respondents indicate that more resources and training on resiliency was needed.

Modeling and Simulation

Five cases of port disruption, in terms of the impacts on waterside and landside capacities, have been considered: 1) Closure of Galveston Channel due to an oil spill, 2) Closure of Port of New York and New Jersey due to Hurricane Sandy, 3) Simulated partial closure of Port Everglades due to flooding, 4) Simulated oil/bio-hazard spill at the Port of New Orleans, 5) Labor strike at the Port of Long Beach. These cases were described in the previous annual report. The first two, involving actual disruptions that took place, will serve to validate the tool. During Year 3, in completing the tool, consideration was given to modeling complexities in port operations, involving type of cargo and dynamic interactions between various logistics components such as handling, transportation and storage, with the primary objective of maximizing stakeholder value. These complexities impact the simulations and hence assessment of port resiliency.

Due to the volume of the data needed to develop the Monte Carlo simulation of the three ports (Port Everglades, Port of New Orleans and Port of Long Beach), 12 months of AIS data from each port was purchased from MarineTraffic.com. The data contains 160,180 records of vessel arrivals, departures, and dwell time starting July 1st, 2015 and ending June 30th, 2016. For all practical purposes, this data is identical to that provided by the U.S. Army Corps of Engineers (USACE) described earlier. The vessel data was analyzed to identify probability distributions of vessel arrivals and dwell time by cargo type and time of day. Partial details are provided below for cargo considerations undertaken for Port Everglades.

Broadly, the Monte Carlo simulation for the Port Everglades was accomplished in three primary tasks. The first task was grouping vessels into general categories based on cargo type. The second task was to generate probability distribution functions (PDF) and cumulative probability distribution functions (CDF) from vessel arrivals and dwell times. The third task was to use the Inverse Transforms Sampling approach to generate random vessel arrivals and departures (arrival time plus dwell time) to match the observed distributions. The fourth task was the validation of the model results. The following sections describe these tasks and their respective results in further detail.

Vessel Categorization by Cargo Type

The underlying assumption of the Monte Carol simulation was that vessels carrying similar cargo, had similar arrival and dwell time patterns. With this assumption, stratifying the vessels based on cargo type yields a more realistic simulation. Table 1 shows vessel types, the number of observed arrivals in the sample, the mean gross tonnage, mean dead weight tonnage, and mean draught of each category.

Table 1: Port Everglades Vessel Types

Cargo Type:	Num. Arrivals:	AVG. GT	AVG. DWT	AVG. DRAUGTH
Fuel/Chemical/Hazard	350	29,865	49,269	88
Construction Material	16	8,298	11,417	58
Vehicles	70	21,103	9,304	66
Heavy-Load Carrier	647	1,460	1,565	47
Passenger	728	104,191	10,161	75
Other Cargo	2,292	16,807	20,604	69

Vessel Arrivals

With the data stratified by cargo type, frequency distribution plots for the arrival times were developed. For simplicity, vessel arrivals were categorized into one hour bins, i.e., if a vessel arrived at 4:25 AM, then it was counted in the 4:00 AM – 5:00 AM bin. This approach was taken for all cargo types and all hours of the day. The next step was to divide the number of arrivals in each bin by the total number of arrivals, thereby providing the proportion of the vessels that arrived during any hour of the day. These data led to the development of the associated probability distribution function (PDF). Next, the integral of the PDF was taken to generate the cumulative probability distribution function (CDF). The vessel arrival PDF and CDF for vessel Fuel/Chemical/Hazard was representative of most vessel entries into the port and serves as a general example in Figure 1 and 2.

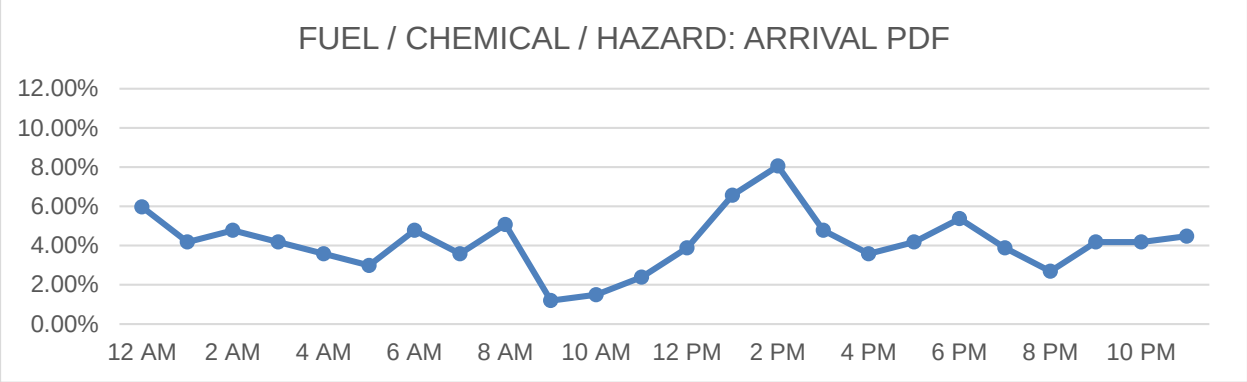


Figure 1: Fuel / Chemical / Hazard Arrival PDF

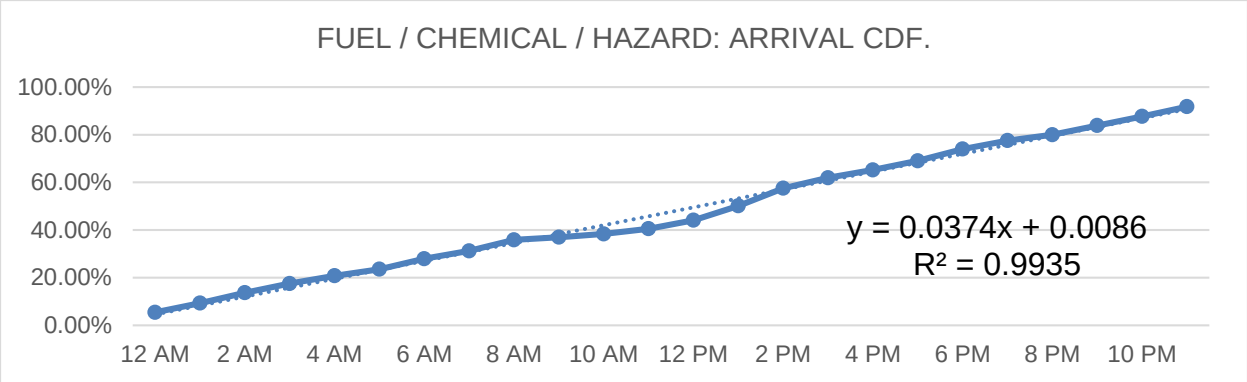


Figure 2: Fuel / Chemical / Hazard Arrival CDF

These figures indicated that vessel arrivals were approximately uniform in their distribution. Investigating the CDF, the trend line and subsequent R^2 value reinforces the suggestion that the PDF is uniformly distributed. A flat, perfect uniform distribution has an integral that is perfectly linear. The R^2 value for the linear trend line in the CDF of Figure 1 was 0.9935, indicative of an excellent linear approximation. This pattern of arrival was seen in most vessel types. Passenger vessels, such as cruise ships had a distinctive arrival PDF and CDF which was more closely related to a normal distribution for the PDF with a sigmoidal shape of the CDF as shown in Figures 3 and 4.

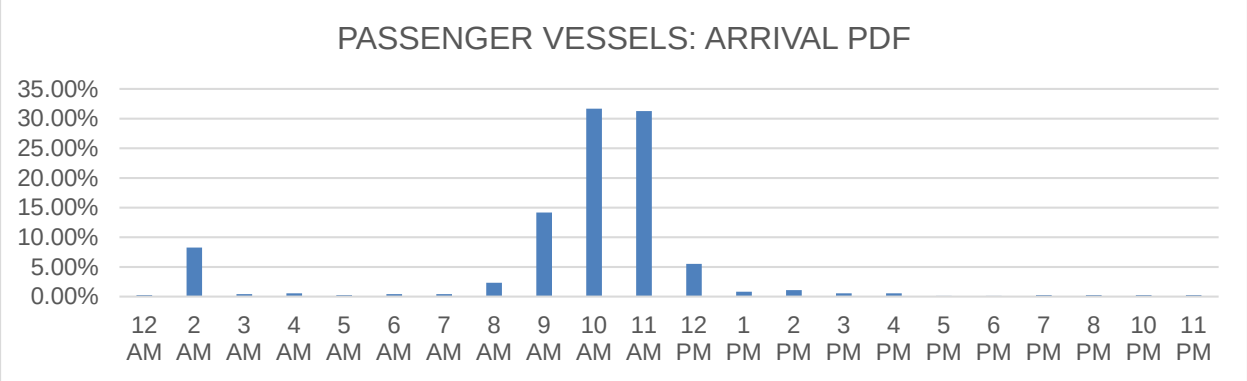


Figure 3: Passenger Vessels Arrival PDF

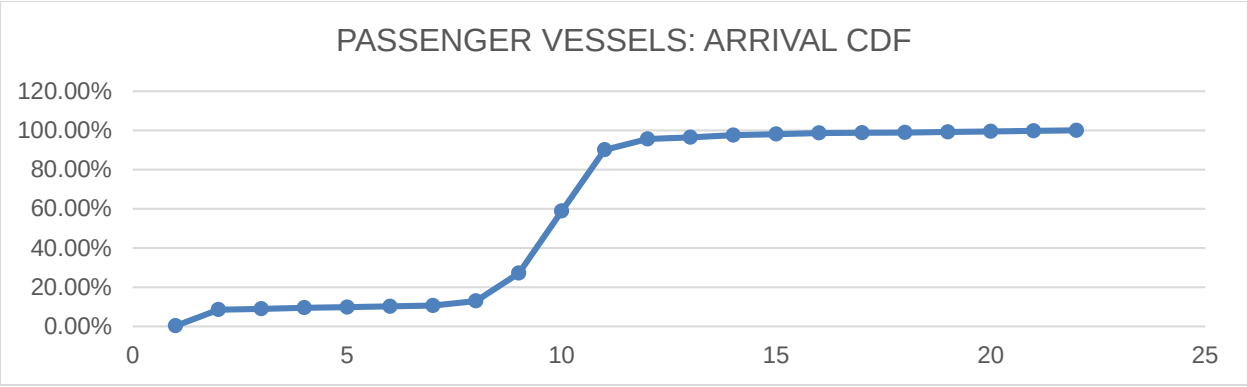


Figure 4: Passenger Vessels Arrival CDF

To simulate vessels arrivals the Inverse Transform Sampling method was applied. Fundamentally, this approach uses the inverse of the CDF plot to transform a uniformly distributed random value into vessel arrivals, which match the observed distribution function. From the CDF plot, every hour represented a range of probabilities. For instance, referencing Figure 3, the hours of 7AM to 8AM covered a range of probabilities between approximately 34 percent and 39 percent. Uniformly distributed random numbers between zero and one were generated for every hour of the day and every day of the year, for one year. If the random number fell between the ranges specified in the CDF for that hour, then a vessel of that particular cargo type was generated. Going back to the example, if the random number generated during the 7AM to 8AM interval was between 0.34 and 0.39, then a Fuel/Chemical/Hazard vessel was generated in the simulation model during that time interval for that day. Figures 5 and 6 show the simulated vessel arrival PDF and CDF for Fuel/Chemical/Hazard cargo vessels. These figures correspond to the PDF and CDF shown in Figures 3 and 4, respectively.

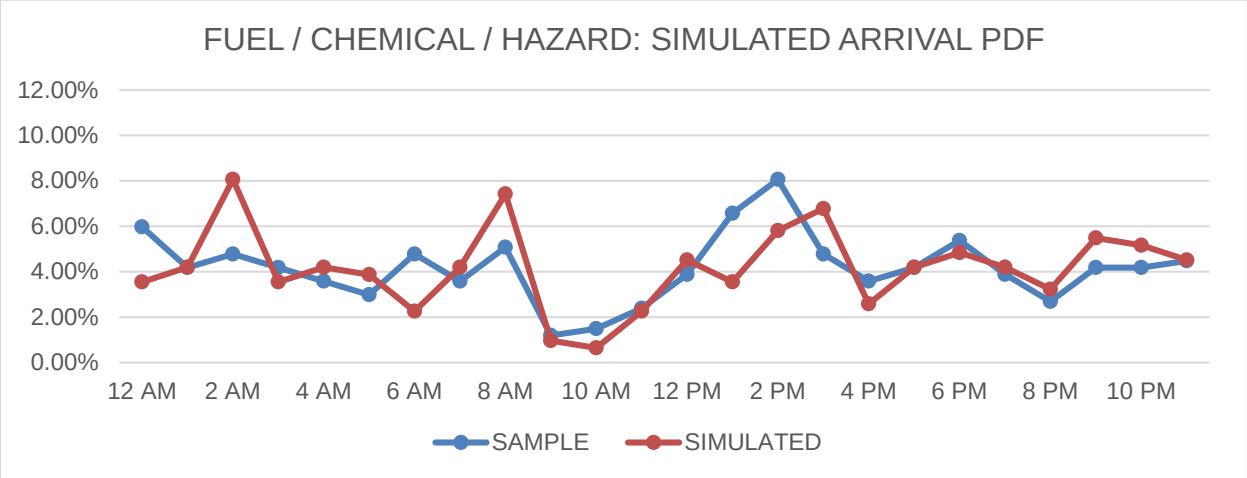


Figure 5: Fuel / Chemical / Hazard Simulated Arrival PDF

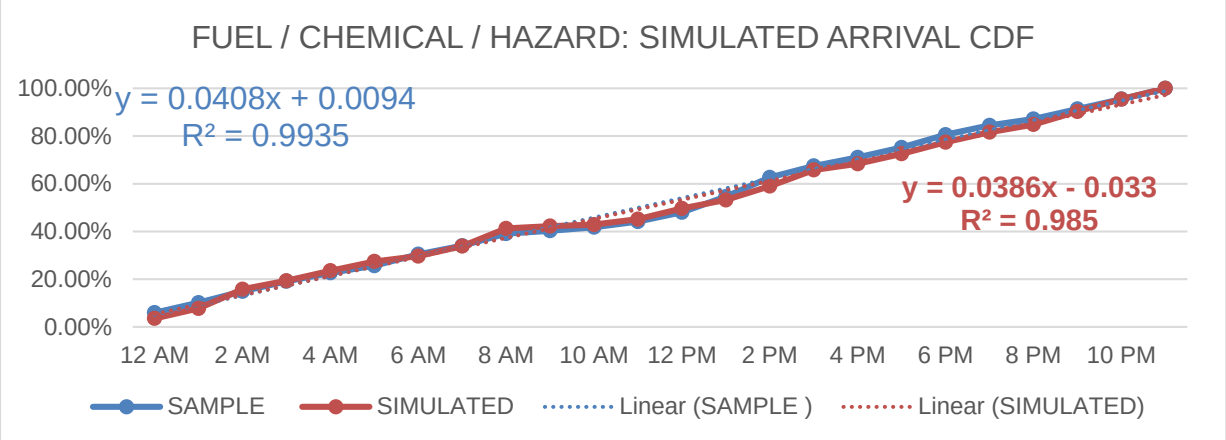


Figure 6: Fuel / Chemical / Hazard Simulated Arrival PDF

Vessel Dwell Times

Vessel dwell times were also simulated using the Inverse Transform Sampling approach. From the dwell time PDF plots, it became apparent that each cargo type had a unique distribution. For example, the Fuel/Chemical/Hazard suggested the dwell times was normally distributed while, Construction Materials was uniformly distributed. Passenger vessels dwell times also showed signs of a normally distributed PDF but, was uniquely different from that for the Fuel/Chemical/Hazards vessels. Vehicle cargo and Heavy-Load Carriers was logarithmically distributed but again these distributions were uniquely different.

Fundamentally, the data suggested that each cargo type has unique processing characteristics which closely follows known distribution types. From a modeling perspective, this is advantageous because unlike vessel arrivals, vessel dwell time is a continuous variable and calculating the CDF or integral could prove challenging if irregular functions are discovered. Therefore, curves were fitted to the PDFs of each cargo type and the Monte Carlo models built based on these fitted curves. Using the Inverse Transforms Sampling method, the integral of the fitted PDF curves was calculated (the CDF) and the inverse was taken to generate random vessel dwell times from these fitted distributions. Table 2 shows the distribution type and equations for the PDF, CDF, and Monte Carlo simulation model for various vessel types. Figures 7 and 8 show the simulated sample dwell times, their fitted distribution curves, and the simulated dwell time PDF and CDF, respectively.

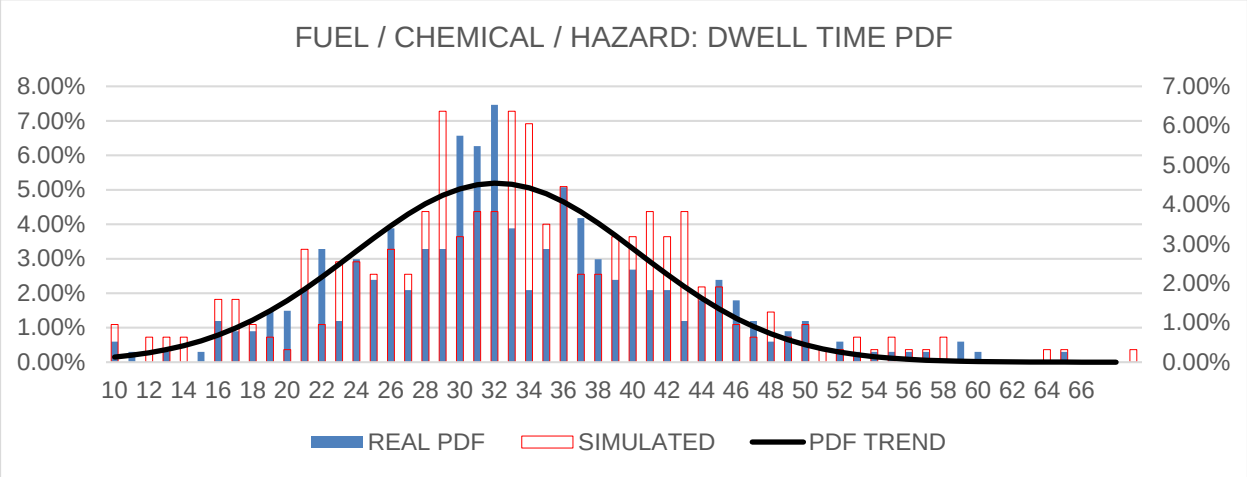


Figure 7: Fuel/Chemical/Hazard Dwell Time PDF

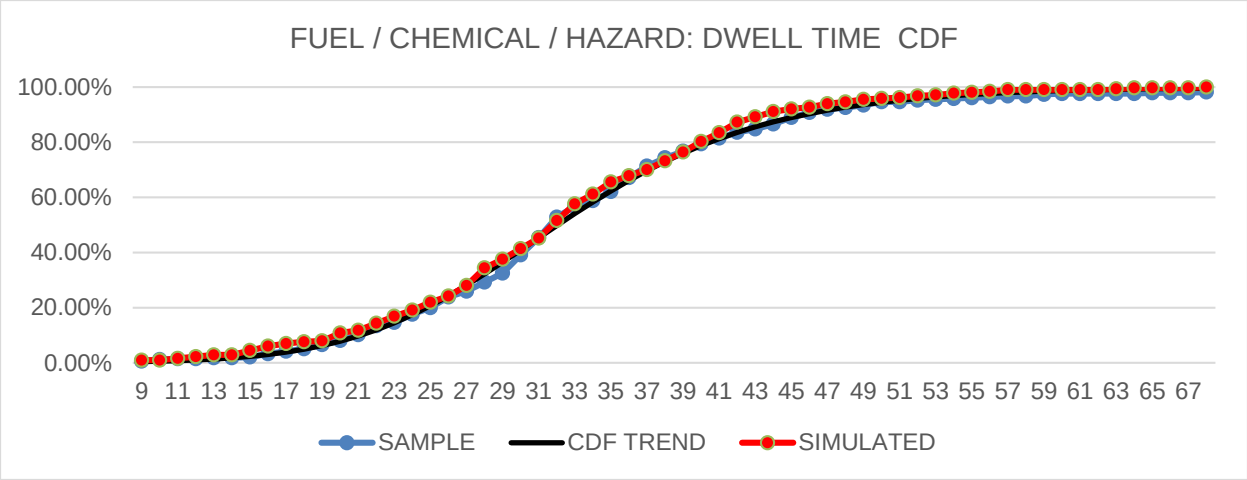


Figure 8: Fuel/Chemical/Hazard Dwell Time CDF

Table 2: Dwell Time Distributions and Monte Carlo Models

Cargo Type:	Distribution Type:	PDF	CDF	Model
Fuel/Chemical/Hazard	Normal	$\hat{y} = 0.045e^{-\left[\frac{(x-32.1)^2}{2(8.3)^2}\right]}$	$\int \hat{y}\,dx = \left[1 + e^{-0.15[x-25.55]}\right]^{-2.14}$	$\left[\int \hat{y}\,dx\right]^{-1} = \frac{\ln\left[\left(\frac{1}{x}\right)^{\frac{1}{2.14}} - 1\right]}{-0.15} + 25.55$
Construction Material	Uniform	$\hat{y} = 0.02439$	$\int \hat{y}\,dx = 0.0243x - 0.0211$	$\left[\int \hat{y}\,dx\right]^{-1} = \frac{x + 0.0211}{0.233}$
Vehicles	Logarithmic	$\hat{y} = [2.806\ln(x + 1.09)]^{-1.963}$	$\int \hat{y}\,dx = [0.281\ Ln(x + 1.157)]^{0.966}$	$\left[\int \hat{y}\,dx\right]^{-1} = e^{\frac{\frac{1}{x^{0.966}}}{0.282}} - 1.09$
Heavy-Load Carrier	Logarithmic	$\hat{y} = [1.07\ln(x + 1.729)]^{-5.753}$	$\int \hat{y}\,dx = [0.271\ Ln(x + 0.232)]^{0.139}$	$\left[\int \hat{y}\,dx\right]^{-1} = e^{\frac{x^{1/0.139}}{0.271}} - 0.232$
Passenger	Beta	Under Development	Under Development	Under Development
Other Cargo	Exponential	Under Development	Under Development	Under Development

Publications

- *Port Resiliency Study*. M. Dhanak, E. Kaisar, A. Sapat, S. Parr, and B. Wolshon. A brief provided to the Area Maritime Security Committee, Dania Beach Florida, August, 2016
- *"Simulation-based Port Resiliency Planning and Assessment Tool".* M. Dhanak, E. Kaisar, A. Sapat, S. Parr, and B. Wolshon. Presentation made at the Workshop on Enhancing Port Resiliency, FAU, December 2016.
- Peer-reviewed conference and journal papers in preparation.

Acknowledgements

Fruitful discussions were held with USCG R&D Center and with USCG Sector Miami personnel. The authors acknowledge the Gulf Coast Center for Evacuation and Transportation Resiliency; a United States Department of Transportation sponsored University Transportation Center at Louisiana State University and a member of the University of Arkansas's Maritime Research and Education Center (MarTREC). The authors also recognize the support of Mr. Steve Nerheim of the Houston-Galveston Vessel Traffic Service (VTS) who was instrumental in compiling and explaining the channel closure data used in this study. Continuing discussions with Port Everglades are acknowledged.

2.3. Maritime Cyber Security

2.3.1. Overview

In July of 2016, this project started and has focused on six separate topic areas as shown in Table 1.

Table 1. Research Topics and Questions

Topic Area		Research Questions
1	Risk-Based Performance Standards	What risk-based performance standards can be developed for cyber risk management of the Marine Transportation System (MTS)? How would performance standards inter-relate with other infrastructure sectors and their performance standards? How would performance standards inter-relate with existing safety and security management systems?
2	Framework for Cyber Policy	What type of criteria should be utilized to develop an academically rigorous framework for Cyber Policy for the MTS?
3	Critical Points of Failure	Based on a multi-node analysis, what are the critical Points of Failure within the cyber system supporting the MTS?
4	Requirements for Maritime Cyber Range	What are the critical requirements that should be considered when developing an academically rigorous and multi-use Maritime Cyber Range?
5	Framework for Point of Failure Detection Methodology	What methodologies can be utilized or invented to develop a framework to analyze a point of Failure Detection Methodology?
6	Maritime Cyber Deterrent Strategy Effectiveness	What methodologies can be employed to conduct a quantitative analysis of maritime cyber deterrent strategy effectiveness?

Over the course of the project, the team will perform and document new research across all six topic areas. This report contains the results associated with the following topics completed during the first year of the project:

- Topic Area 1: Risk-Based Performance Standards.
- Topic Area 2: Framework for Cyber Policy
- Topic Area 3: Framework for Point of Failure Detection Methodology

2.3.2. Intended Customers

The primary intended customers for this research are the broad range of government stakeholders with cybersecurity roles and responsibilities, specifically:

- United States Coast Guard (USCG) and Department of Homeland Security (DHS) headquarters (HQ) offices responsible for the development of cybersecurity-related regulations, policies, and communications:
  - Assistant Commandant for Prevention Policy (CG-5P)
  - Port & Facility Compliance (CG-FAC)
  - Design & Engineering Standards (CG-ENG)
  - Standards Evaluation & Development (CG-REG)
  - Cyber Command (CGCYBERCOM)
  - DHS Office of Cybersecurity and Communications (CS&C)

- USCG Area, District, and Sector units responsible for interacting with industry to provide awareness of cyber concerns and government cybersecurity-related policy
- USCG and DHS centers who perform research in maritime cyber security:
  - Research & Development Center (CG-RDC)
  - DHS Science & Technology (S&T) Cyber Security Division

- Other DHS and USCG HQ offices with roles associated with maritime cyber security
  - Domestic Port Security Evaluation Division (CG-PSA-2)
  - Investigations & Analysis (CG-INV)
  - Commercial Vessel Compliance (CG-CVC)
  - Operating & Environmental Standards (CG-OES)
  - Cyber & Intelligence Forces (CG-791)
  - DHS Infrastructure Security Compliance Division (ISCD)

2.3.3. Intended Processes

The research is intended to inform government stakeholders in the development of cybersecurity-related regulations and policies. In addition, the research should support interactions with industry to improve awareness of cyber threats and provide actionable guidance to improve cybersecurity by addressing vulnerabilities.

2.3.4. Project Objectives and Guiding Principles

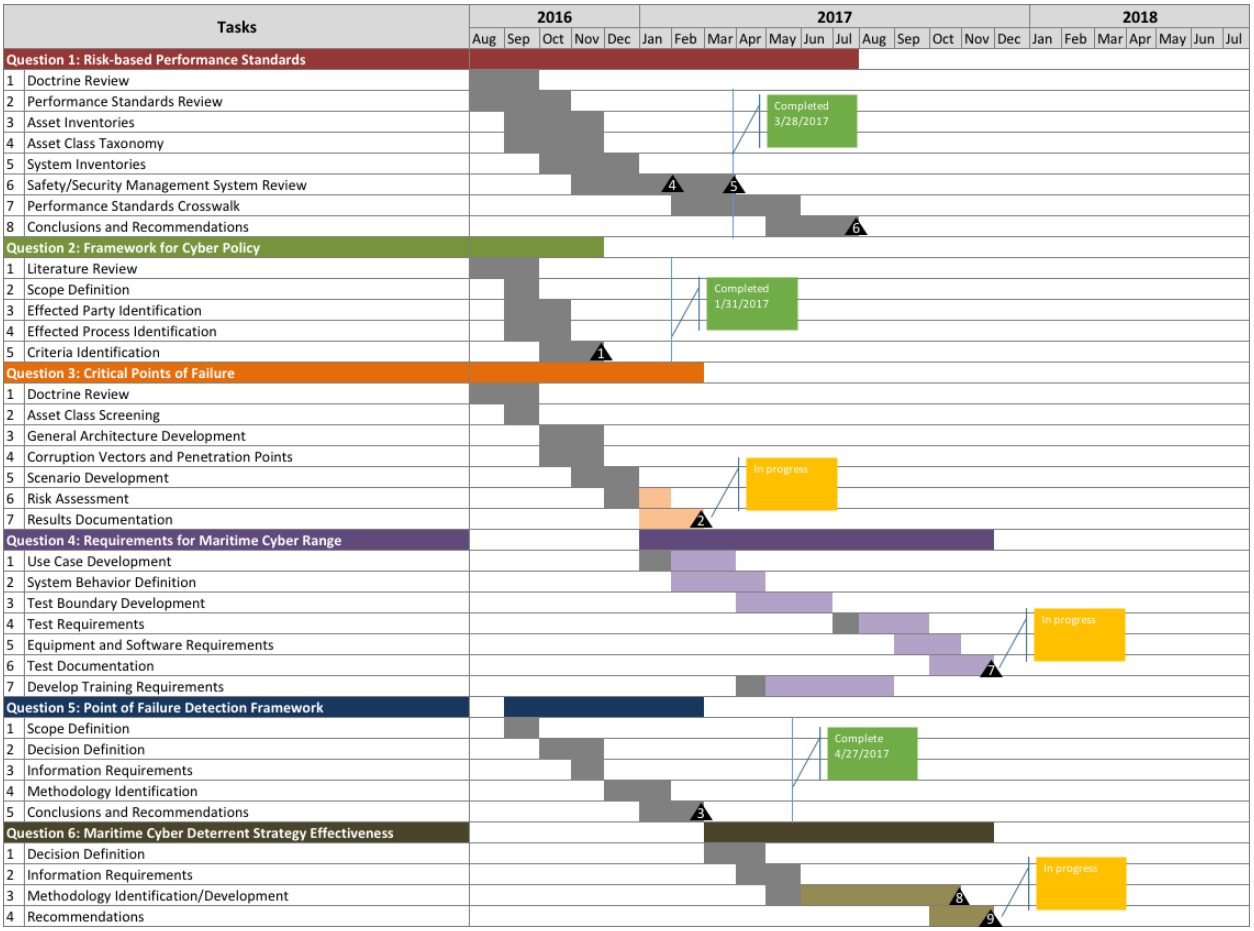
The research is intended to inform government stakeholders in the development of cybersecurity-related regulations and policies. In addition, the research should support interactions with industry to improve awareness of cyber threats and provide actionable

guidance to improve cybersecurity by addressing vulnerabilities. In the performance of this project, the research team was guided by the following principles:

- Strong collaboration with Stevens Institute of Technology and government stake-holders to ensure that the deliverables are addressing key areas of need
- Leverage established standards and guidance to ensure that the products are academically rigorous and address the scope of maritime industries and assets
- Develop practical products tailored to the intended audiences and processes
- Actionable, understandable, and backed by evidence

2.3.5. Milestones

The original project plan was based on a two-year timetable, however, given the topic of cybersecurity and the rate at which it changes, we are managing the project on a stretch goal of completion in 16 months. The following outlines our planned, in-progress, and completed research tasks through the end of the project.



2.3.6. Background - U.S. Maritime Transportation System

The MTS is instantiated through a diverse set of ports and waterways throughout the U.S. Each port is different with unique geographic and hydrographic features as well as a unique mix of industries and operators. There are a wide variety of users within the MTS, including: facility owner/operators, domestic vessel operators, foreign vessel operators, public boaters, military, and federal/state/local government agencies.

From a systems perspective, the MTS has a network of maritime operations that interface with shore side operations at intermodal connections as part of global supply chain and domestic commercial operations. The MTS includes international and domestic passenger transportation (ferry and cruise) operations that connects to other forms of passenger transportation through U.S. ports. There are many types of infrastructure, including: bridges, tunnels, dams, locks, levees, power plants, and pipelines, that are part of or border on the MTS. Furthermore, the MTS includes recreational use by a large, nationwide boating community and use by military and other government vessels to carry out their missions. Finally, there are thousands of commercial waterfront facilities, attractions, and buildings that are not explicitly part of the MTS, but which can impact MTS operations.

Figure 1 provides an example representation of a port, highlighting the MTS components.

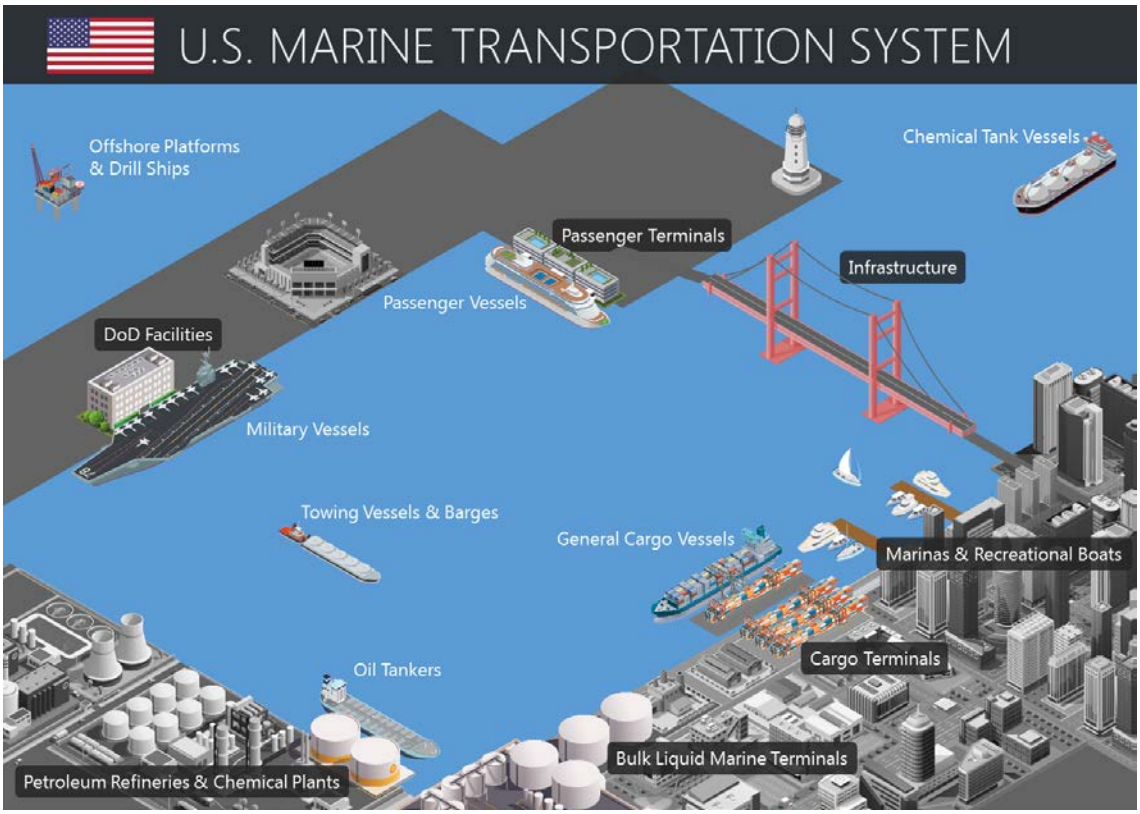


Figure 1. Example Port with Common MTS Component

2.3.7. Analytical Scope

Assessing cyber vulnerabilities and consequences for a system as complex as the U.S. MTS is inherently difficult. The industries and assets operating within the MTS are broad and diverse, and the array of cyber threats are innumerable and evolving. Adversaries have a wide range of capabilities and objectives in their attacks. To help focus on the most important areas, the research team worked with project sponsors and stakeholders from the USCG and DHS to define analytical boundaries of this research. The research team will primarily focus on cyber scenarios involving MTS assets' technology systems that, if compromised, could result in physical consequences (e.g., deaths, injuries, spills, property damage, port commerce impacts). The team will also consider cyber-attacks employed in concert with physical attacks to increase the probability of attack success or consequences.

The study will not address cyber scenarios focused solely on impacting businesses, such as through the theft of propriety business data or the disruption of business systems. The following sections further refine the team's analytical scope by exploring a variety of scenario attributes.

Section 1: Asset Classes

The team will focus its research on asset classes that typically operate within the U.S. MTS, including: vessels, barges, facilities, and offshore platforms. The primary focus will be on assets that are regulated under the U.S. Maritime Transportation Security Act (MTSA)[1] or the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS), specifically:

- U.S. flagged vessels (MTSA, Part 104)
- Foreign flagged vessels (ISPS)
- Facilities (MTSA, Part 105)
- Offshore platforms (MTSA, Part 106)

In addition, the team will evaluate the following asset classes that are not regulated under MTSA, but if compromised, could significantly impact MTS operations:

- Maritime infrastructure (e.g., bridges, dams/locks)
- Smaller commercial vessels (e.g., tugs, fishing boats)
- Maritime facilities (e.g., marinas)

The following asset classes are out of scope for this research project:

- Military facilities and vessels

[1] https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

- Government systems related to the MTS (e.g., vessel traffic system, automated identification system)
- Recreational boats
- Non-maritime commercial assets that border the MTS (e.g., stadiums, attractions, buildings)
- Water crossings (e.g., pipelines, cables)
- Non-maritime infrastructure that border the MTS (e.g., waterside power plants)

Systems

This research project will consider exploitation of both information technology (IT) and operational technology (OT) systems.

Gartner defines information technology (IT)[2] as *the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.* Gartner defines operational technology (OT)[3] as *hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise*. OT includes industrial controls systems (ICSs), and section 2 of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82[4] provides a useful overview of ICSs:

> *ICS, which is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). The part of the system primarily concerned with producing the output is referred to as the process. The control part of the system includes the specification of the desired output or performance. Control can be fully automated or may include a human in the loop. Systems can be configured to operate open-loop, closed-loop, and manual mode. In open-loop control systems the output is controlled by established settings. In closed-loop control systems, the output has an effect on the input in such a way as to maintain the desired objective. In manual mode the system is controlled completely by humans. The part of the system primarily concerned with maintaining conformance with specifications is referred to as the controller (or control). A typical ICS may contain numerous control loops, Human Machine Interfaces (HMIs), and remote diagnostics and maintenance tools built using an array of network protocols.*

[2] http://www.gartner.com/it-glossary/it-information-technology/
[3] http://www.gartner.com/it-glossary/operational-technology-ot/
[4] http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf

IT and OT systems are very different. They exist for different purposes, use different technologies, and protocols. They also have very different consequences if they fail. Scenarios involving IT system exploitation are likely to impact business communications or the confidentiality of data. Successful attacks can impact a company's bottom line, compromise private information, or effect the performance of a variety of key business functions. Examples of high-profile IT system scenarios include:

- **Email hacks** on the Democratic National Committee and Sony Pictures
- **Major data breaches** from Target, Yahoo, and U.S. Office of Personnel Management
- **Ransomware** attacks against numerous U.S. hospitals
- **Denial of Service** attacks against GitHub, the British Broadcasting Corporation, and Facebook

OT failures can result in the loss of control of operational processes, which can result in economic impacts, physical consequences, structural damage to equipment or facilities, and environmental ramifications. Examples of high-profile OT scenarios include:

- **Equipment damage** due to Stuxnet malicious worm causing Programmable Logic Controllers (PLCs) within Iran's nuclear centrifuges to spin too quickly and tear themselves apart.
- **Safety issue** when a diver tender station-keeping system on an offshore asset "blue screened" and drifted away, severing the diver umbilical.
- **Operation downtime** when tidal turbine was hacked and its operating software was encrypted. The utility was held for ransom resulting in a 15-day delay.
- **Property damage** when a German steel mill's Industrial Control System (ICS) was hacked, disabling the ability to shut down a blast furnace and subsequently resulting in an explosion causing major damage to the facility.

Because they exist for different purposes, IT and OT systems have nearly the opposite priorities. OT systems emphasize availability, integrity, and confidentiality in that order, whereas, IT prioritizes confidentiality, then integrity, and then availability.
Consider the following availability example: Does a 1-minute delay in an IT email server's performance result in serious consequences? No. Whereas, a 1-minute delay in an OT system signal can cause process impacts leading to: equipment damage, safety issues, environmental spills, product loss, or critical mission delays.

Historically, OT systems have often been isolated, whether virtually or physically, from IT networks. OT systems are often managed by engineering or operations departments that are primarily concerned with ensuring that the systems are "up-and-running" and maintaining control over operations. These systems are designed to be simple and reliable with a much longer lifespan (e.g., 30 years) when compared to IT systems (e.g., 6-10 years). The isolation of OT has traditionally been viewed as the ultimate safeguard against outside threats, but the days of OT isolation are coming to an end.

There are a number of emerging business needs to integrate OT with IT systems to improve operational efficiency to remain competitive, such as:

- **Enterprise Resource Planning (ERP).** Passing data between OT and ERP IT systems to support a variety of business functions, including: supply chain management, inventory control, and customer billing, while reducing costs and redundant tasks, such as duplicate data entry.
- **Vessel Routing and Fuel Management Systems.** Monitoring and reporting fuel consumption data and performing analytics to optimize fuel usage to increase operational efficiency.
- **Software Upgrades.** Providing remote access to vendors to enable software management to minimize cost and downtime.
- **Predictive Maintenance.** Condition monitoring of equipment to proactively identify potential failures to inform predictive maintenance activities.

Many companies are beginning to weigh the pros and cons of IT/OT integration, but many see this integration as inevitable. Since OT system exploitation is far more likely to result in the physical consequences, the team will focus on OT system exploitation scenarios. IT system exploitation will primarily be considered only as a potential threat vector to OT systems, if the systems are integrated. Figure 2 provides examples of common IT/OT components and introduces issues and challenges associated with an enterprise's cybersecurity for both IT/OT systems.

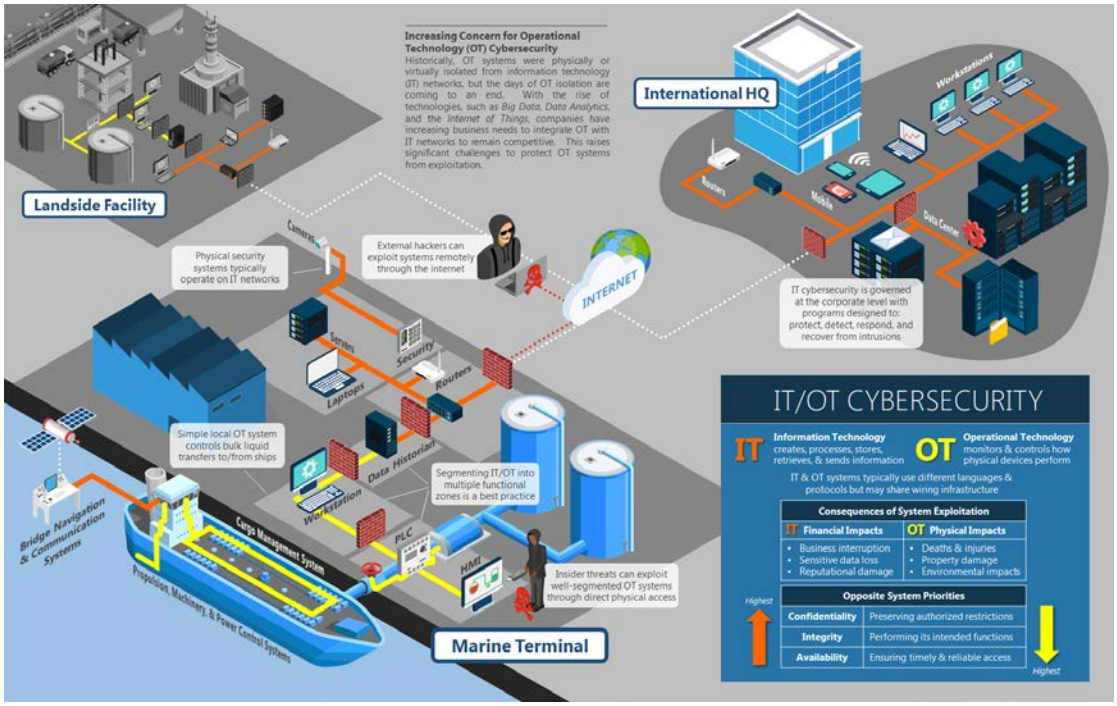


Figure 2. IT/OT Cybersecurity Overview

Threats

The research team will consider two major threat categories to IT and OT systems: **Cybersecurity** threats involve the intentional disruption or exploitation of a computer network or control system by adversaries. The skills and techniques of the adversaries can vary dramatically from low-level hackers to Advanced Persistent Threats (APTs) with coordinated attacks by organized crime or nation states. APTs are decidedly more capable in assembling a multidisciplinary team with the full set of knowledge and skills necessary to carry out the attack. **Cybersafety** threats involve the accidental corruption or misuse of cyber systems by owner/operator personnel or third parties, such as vendors or guests.

Vulnerabilities

The team considered a wide variety of potential system vulnerabilities spanning several areas and disciplines. For consistent accounting and communication of vulnerabilities, team will leverage the vulnerability or predisposing condition taxonomy from Appendix C of NIST SP 800-82. The major categories are:

- Policy and procedure
- Architecture and design
- Configuration and maintenance
- Physical
- Software development
- Communication and network configuration

Consequences

The traditional emphasis of cybersecurity has been IT-focused: prevention of proprietary/personal information theft and ensuring the integrity of business systems (e.g., corporate Websites, accounting systems). This project is focused on scenarios that could result in or contribute to physical consequences. Specifically, the team will focus on scenarios that could result in or contribute to a security incident resulting in a significant loss of life, environmental damage, or disruption to the MTS.

Section 2: Common IT/OT Systems

The first section of this report introduced the many different classes of assets that operate in the U.S. MTS. Due to the wide range of missions and activities performed by these assets, it should be no surprise that there is a vast collection of diverse IT and OT systems employed to support these functions. The roles of the systems are diverse: mission-specific control functions, security systems, communications, and business. The assortment of systems is increasing each year as automation becomes more ubiquitous and manual functions are replaced or augmented by systems.

Vessel Systems

The literature references that are specifically associated with vessels, BIMCO (Table 4, Reference #9), IMO (Table 4, Reference #10), and ABS (Table 4, Reference #11), each provide a list or table of common vessel systems. The research team reviewed each of these references, read other publicly available sources, and interviewed maritime experts to develop a simple consolidated list of vessel systems (Table 2). This list is not comprehensive, but is meant to represent the range of IT/OT systems that is commonly found on commercial vessels.

Table 2. Common Vessel Systems

Communication Systems
Satellite Communication Equipment
Voice Over Internet Protocols (VOIP) Equipment
Wireless Local Area Network (WLAN)
Public Address and General Alarm Systems
Bridge Systems
Positioning Systems
Electronic Chart Display Information System
Automatic Identification System (AIS)
Global Maritime Distress & Safety System (GMDSS)
Radar Equipment
Voyage Data Recorders (VDRs)
Cargo Management Systems
Propulsion, Machinery, & Power Control Systems
Alarm System
Emergency Response System

Access Control Systems
Surveillance Systems
Bridge Navigational Watch Alarm System
Shipboard Security Alarm Systems
Electronic “Personnel-On-Board” Systems
Passenger Servicing And Management Systems
Property Management System (PMS)
Medical Records
Ship Passenger/Seafarer Boarding Access Systems
Passenger-Facing Networks
Passenger Wi-Fi or LAN Internet Access
Guest Entertainment Systems
Communication
Core Infrastructure Systems
Administrative & Crew Welfare Systems
Administrative Systems
Crew Wi-Fi Or LAN

Facility/Infrastructure Systems

The research team reviewed numerous publicly available sources and held discussions with numerous internal facility experts to develop a simple consolidated list of systems commonly found at maritime facilities and infrastructure components (Table 3). Again, this list is not comprehensive, but is meant to represent the range of IT and OT systems that is commonly found at facilities and infrastructure.

Table 3. Common Facility/Infrastructure Systems

Operational Control Systems
Distributed Control Systems
Ramp Control Systems
Terminal Operating Systems
Independent Safety Systems
Alarm Systems
Fire Protection Systems
Environmental Protection Systems (Spill Control)
Emergency Shut Down Systems
Building Management Control Systems
Building Automation Systems
Vertical Transport System (Elevators and Escalators)
Interior Lighting Control Systems
Digital Video Management Systems
Energy Management Systems
Exterior Lighting Control Systems
HVAC Systems
Building Safety Systems
Fire Alarm Systems
Fire Sprinkler Systems
Gas Detectors
Public Safety/Land Mobile Radios
Smoke And Purge Systems
Emergency Management Systems
Security Systems
Physical Access Control Systems
Intrusion Detection Systems
Surveillance Systems
Screening Systems
Police Dispatch

Miscellaneous Systems
Digital Signage Systems
Laboratory Instrument Control Systems
Renewable Energy Geothermal Systems
Renewable Energy Photo Voltaic Systems
Shade Control Systems
Advanced Metering Infrastructure
Business Systems
Passenger Check-In Systems
Telecommunication
Email
E-Commerce
Enterprise Resource Planning
Sales
Procurement
Inventory Control
Production
Distribution
Accounting
Human Resource
Performance Management
Custom Relationship Management
Enterprise Asset Management
Business Intelligence

2.3.8. Literature Review

The team performed a broad literature review of authoritative sources related to maritime and critical infrastructure cybersecurity to inform execution of this project. USCG and DHS stakeholders identified several references to review.

USCG Rear Admiral Paul Thomas (CG-5P) has stressed the importance of and USCG's commitment to the use of national and international standards, such as the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, the Department of Energy's (DOE's) *Cybersecurity Capability Maturity Model (C2M2)*, various International Organization for Standardization (ISO) standards, and others[5]. Because of the international and cross-industry nature of the MTS, an overarching framework, specifically, the NIST Framework, must be used as a basis to realize any practical application and acceptance of cyber policy. The NIST Framework which provides mapping to several recognized standards is the central reference for this work. Table 4 documents the collection of references that were reviewed.

Table 4. Literature Review

#	Organization	Title	Release Date
1	NIST	*Framework for Improving Critical Infrastructure Cybersecurity*	February 2014
2	NIST	SP 800-82 Revision 2, *Guide to Industrial Control Systems Security*	February 2015
3	ISO	ISO 27001: *Information Security Management Standard* (Link not available)	October 2013
4	DOE / DHS	*C2M2*	February 2014
5	ISA / IEC	*Industrial Network and System Security* (ISA 62443) (Link not available)	November 2011
6	NIST	SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	February 2005
7	DoD	Instruction 8500.01, *Cybersecurity*	March 2014
8	DHS	*Transportation Systems Sector Cybersecurity Framework Implementation Guidance*	June 2015
9	BIMCO	*The Guidelines on Cyber Security Onboard Ships*	February 2016
10	IMO	*Interim Guidelines on Maritime Cyber Risk Management*	June 2016
11	ABS	*Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations*	September 2016

[5] U.S. Congress, House. Committee on Homeland Security. Border & Maritime Security Subcommittee. *Testimony of Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy, on Cybersecurity in U.S. Ports*, *Oct. 8, 2015*

#	Organization	Title	Release Date
12	COBIT 5	Control Objectives for Information & Related Technology (COBIT) 5 *A Business Framework for the Governance and Management of Enterprise IT*	April 2012
13	Council on CyberSecurity	*Top 20 Critical Security Controls (CSC)*	August 2016
14	NIST	SP 800-160, *Systems Security Engineering*	May 2016
15		*USCG Cyber Strategy*	June 2015
16		*National Strategy for Trusted Identities in Cyberspace (NSTIC)*	April 2011
17	NIST	*Maritime Bulk Liquids Transfer Cybersecurity Framework Profile*	November 2016

The set of references listed in Table 4 were created for a range of purposes and audiences; so, to help stakeholders better understand the scope, nature, and potential applications of each reference, the research team provided summaries for all references in Table 5, which includes:

- Basic document attributes: title, authoring organization, release date, document type, and page count
- Applicability to: IT/OT systems, government/commercial, U.S./International, and Facilities, Vessels, & Offshore
- Relative percentage of content (based on page count percentage) focused on providing understanding of cybersecurity issues vs. providing implementation guidance to improve
- High-level description of the contents
- Research team commentary on application to the project

For illustrative purposes of the annual report, included below in Table 5 is one (of 17) document reviews. Please see Appendix C-1 for additional document reviews:

Table 5. Reference Summaries

#1. Framework for Improving Critical Infrastructure Cybersecurity			
Organization	NIST	**Release Date**	February 2014
Type	Framework	**Page Count**	41
Audience	C-level executives, upper- and mid-level operations managers, implementation teams, assessors, consultants, and others interested in understanding the cybersecurity domain		
Content Focus			

Applicability			
Primary Domains	Stakeholders	Geography	Asset Types
✓ IT ✓ OT	✓ Commercial ✓ Government	✓ U.S. ✓ International	✓ Facilities ✓ Offshore ✓ Vessels

Description

The Framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors. The Core provides detailed guidance for developing individual organizational Profiles. A case-specific Profile is developed by the organization to guide the alignment of its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide an implementable reference model that enables an organization map and measure the relative coverage of its implementation against the cybersecurity Framework. This approach mimics a common closed-loop control system that enables the structured design, implementation, and measurement of a maritime cybersecurity system.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity capabilities sophistication – to uniformly apply risk management principles and best practices to improvement of critical infrastructure security and resilience. The Framework organizes and structures multiple effective cybersecurity standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be applied internationally and serve as a model for international cooperation to strengthen critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, and different risk tolerances. Therefore, how they implement the practices in the Framework will also vary. The Framework is intended to help better manage cybersecurity risks, optimize security investments, and protect critical services.

Commentary

(To review the complete reference summary, please see Appendix C-1)

A graphic summarizing the literature review described in Table 4, can be found in Appendix C-2).

2.3.9. NIST Framework Core Mapping

As mentioned earlier in this report, the NIST Framework is the central reference for this project. The Framework was released in February 2014 and consists of three parts: Framework Core, Framework Profile, and Framework Implementation Tiers. The Framework Core provides a three-level hierarchy of (1) functions, (2) categories, and (3) subcategories that describe common activities for managing cybersecurity risk.

Table 6 introduces the first two levels of the hierarchy.

Table 6. NIST Framework Functions and Categories

Function	Category
Identify (ID)	ID.AM - Asset Management
	ID.BE - Business Environment
	ID.GV - Governance
	ID.RA - Risk Assessment
	ID.RM - Risk Management Strategy
Protect (PR)	PR.AC - Access Control
	PR.AT - Awareness and Training
	PR.DS - Data Security
	PR.IP - Information Protection Processes and Procedures
	PR.MA - Maintenance
	PR.PT - Protective Technology
Detect (DE)	DE.AE - Anomalies and Events
	DE.CM - Security Continuous Monitoring
	DE.DP - Detection Processes
Respond (RS)	RS.RP - Response Planning
	RS.CO - Communications
	RS.AN - Analysis
	RS.MI - Mitigation
	RS.IM - Improvements
Recover (RC)	RC.RP - Recovery Planning
	RC.IM - Improvements
	RC.CO - Communications

To help aid in implementation, NIST mapped six globally recognized standards for cybersecurity to the Framework Core's subcategories (Level 3) providing a cross reference from the Framework Core's subcategory to the associated chapter or section in the mapped reference. The six mapped references were:

- ISO/IEC 27001 (Table 4, Reference #3)
- ISA 62443-2-1:2009 & ISA 62443-3-3:2013 (Table 4, Reference #5)
- NIST SP 800-53 (Table 4, Reference #6)
- COBIT 5 (Table 4, Reference #12)

- CCS CSC (Table 4, Reference #13)

The NIST Framework was intended to be a living document to be updated as industry feedback is provided. The NIST Framework did not map *every* cybersecurity standard (e.g., C2M2, NIST SP 800-82) available at that time, and since then, several additional relevant standards and guidance documents have been released. So, the research team mapped six additional, globally-recognized references to the Framework subcategories:

- NIST 800-82 (Table 4, Reference #2)
- C2M2 (Table 4, Reference #4)
- DHS TSS (Table 4, Reference #8)
- BIMCO (Table 4, Reference #9)
- IMO (Table 4, Reference #10)
- ABS (Table 4, Reference #11)

Table 7 provides a simple, summary heat map of the team's mapping that illustrates the coverage of the references. If the reference addresses the requirements in the Framework Core subcategory, an "x" is included in a green cell. If not, the gray cell is blank. The new references mapped by the team are in the left, dark blue columns while the original NIST mapping are in the right, light blue columns. For the purpose of the annual report, we have truncated the complete mapping.

Table 7. Updated NIST Framework Core Mapping

Function *Category* Subcategory	New Mapping						Original Mapping					
	IMO	BIMCO	ABS	C2M2	NIST 800-82	DHS TSS	CCS CSC	COBIT 5	ISA 62443-2-1	ISA 62443-3-3	ISO/IEC 27001	NIST SP 800-53
Communications												
Asset Management												
ID.AM-1	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ID.AM-2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ID.AM-3	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
ID.AM-4	✓	✓	✓	✓		✓		✓			✓	✓
ID.AM-5	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
ID.AM-6	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
Business Environment												
ID.BE-1	✓	✓	✓	✓	✓	✓		✓			✓	✓
ID.BE-2	✓	✓	✓	✓	✓	✓		✓				✓
ID.BE-3	✓		✓	✓	✓	✓		✓	✓			✓
ID.BE-4	✓	✓	✓	✓	✓	✓					✓	✓
ID.BE-5	✓	✓	✓	✓	✓	✓		✓			✓	✓
Governance												

Function *Category* Subcate-gory	New Mapping						Original Mapping					
	IMO	BIMCO	ABS	C2M2	NIST 800-	DHS TSS	CCS CSC	COBIT 5	ISA 62443-	ISA 62443-	ISO/IEC	NIST SP
ID.GV-1	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
ID.GV-2	✓		✓	✓	✓	✓		✓	✓		✓	✓
ID.GV-3	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓
ID.GV-4	✓	✓	✓	✓	✓	✓		✓	✓			✓
Risk Assessment												
ID.RA-1	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
ID.RA-2	✓	✓	✓	✓	✓	✓			✓		✓	✓
ID.RA-3	✓	✓	✓	✓	✓	✓		✓	✓			✓
ID.RA-4	✓	✓	✓	✓	✓	✓		✓	✓			✓
ID.RA-5	✓	✓	✓	✓	✓	✓		✓			✓	✓
ID.RA-6	✓	✓	✓	✓	✓	✓		✓				✓
Risk Management Strategy												
ID.RM-1	✓	✓	✓	✓	✓	✓		✓	✓			✓
ID.RM-2	✓	✓	✓	✓	✓	✓		✓	✓			✓
ID.RM-3	✓	✓	✓	✓	✓	✓						✓
Protect												
Access Control												
PR.AC-1	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PR.AC-2	✓		✓	✓	✓	✓		✓	✓		✓	✓
PR.AC-3	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
PR.AC-4	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
PR.AC-5	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
Awareness and Training												
PR.AT-1	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
PR.AT-2	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
PR.AT-3	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
PR.AT-4	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
PR.AT-5	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Data Security												
PR.DS-1	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
PR.DS-2	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
PR.DS-3	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
PR.DS-4	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓
PR.DS-5	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
PR.DS-6	✓	✓	✓	✓	✓	✓				✓	✓	✓
PR.DS-7	✓	✓		✓		✓		✓			✓	✓

2.3.10. Recommended Risk-based Performance Standards

There are many relevant widely recognized standards and best practices that are applicable to maritime cybersecurity, but the sheer number of references can make it difficult for organizations to choose the best option(s) for them. This section provides specific recommendations for owners/operators of vessels and maritime facilities that are interested in pursuing the development of certification of a cybersecurity program
The first factor to consider is the maturity of a company's cybersecurity program, which the research team has defined in three major categories:

1. Owner/operator has not yet developed a cybersecurity program
2. Owner/operator has implemented an IT cybersecurity program
3. Owner/operator has implemented an IT/OT cybersecurity program

The following three subsections recommend references for each of these categories, respectively.

Owner/Operator Has Not Yet Developed a Cybersecurity Program

The following listed publications are recommended reading for organizations contemplating the implementation of a cybersecurity program, but are not clear on how to begin. If justification of a program is needed, these documents provide useful insights for program planners. At the executive level, the introductions of the documents are useful for gaining a general understanding of the importance and overall scope of a cybersecurity program. The content of these documents provides guidance for structuring a program, without getting excessively detailed with respect to implementation.

1. **NIST Framework** is designed for use as a strategic reference model and not an implementation model. That is not to say that it cannot be used as an implementation guide – it can. It contains sufficient general cybersecurity implementation content to fill that need. However, its structure and relative simplicity are more suited to a broader understanding of the cybersecurity domain at executive and senior management levels. The publication provides insights on security system design goals/outcomes; program implementation coverage; an approach to comparative analysis of a security implementation against a norm; and implementation baselines that promote and encourage economical development and progressive improvement for a cybersecurity program.

2. **NIST SP 800-82** is arguably the canonical reference for control system cybersecurity in the United States and is a primary resource globally. The length of the publication makes it difficult to approach; however, it is exceptionally well-organized, and its information density is notable. The four-page *Executive Summary* is beneficial for level-setting the natures of cybersecurity issues and solutions. In

addition, the appendices provide a useful desktop reference for navigating the entire NIST SP 800 series.

3. **NIST 800-160** gives evidence that understanding of the cybersecurity is maturing and evolving rapidly. It is an exceptional tutorial on the dependencies of system security on robust system engineering and characterizes cybersecurity as a smaller subset of "systems security engineering," or SSE. Although much of the NIST 800-160 presents implementation activities, the six-page *Forward* and seven-page *Introduction* are recommended reading for all personnel being introduced to cybersecurity.

4. **NSTIC** fills a gap in cybersecurity reference papers by introducing and defining an "Identity Ecosystem." Rigorous identity management of people and machines that are granted cyber access to marine and offshore assets is arguably foundational to cybersecurity; however, the topic receives limited attention in other publications. The publication provides a U.S. strategy for establishing a cyber environment in which organizations can implement secure, efficient, user-friendly, and plug-and-play identity solutions. NSTIC also describes an Identity Ecosystem Framework in which "interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms" can be implemented to improve identity trust to all authorized users and reduce identity proof procedures at the user interfaces.

5. **BIMCO** publication focuses on cybersecurity for cargo and passenger vessels, and therefore limits its cybersecurity discussion to protecting ship handling, cargo management, and passenger support systems as OT systems. The document provides a high-level description of generally accepted best practices and recommendations. These descriptions could be used to outline a cybersecurity program or policy.

Owner/Operator Has Implemented an IT Cybersecurity Program

The following list of references is recommended reading for organizations that have established an IT cybersecurity program, but want additional information on extending the program to purpose-built OT systems (e.g., ICSs). These organizations are advised to also review the references listed above, as well as those listed below:

1. **NIST SP 800-82*** specifically differentiates industrial control systems from IT systems and discusses security solutions for OT. The 67 pages of "implementable" information presented in Appendix G describe OT-related security processes that are especially useful in "tailoring" and may be needed to adjust robust IT security program to accommodate ICS security.

2. **NIST 800-160*** is an exceptional tutorial on the dependencies of system security on robust system engineering and characterizes cybersecurity as a smaller subset of "systems security engineering," or SSE. The concepts and implementation

guidance presented are useful for strengthening an existing IT system security program or developing an OT security program.

3. **ISO/IEC 62443-2-1** provides an overview of the OT cybersecurity domain and detailed cybersecurity management fundamentals as organized as risk recognition/analysis, risk reduction, risk monitoring, and improvement. It further details each category into objectives, descriptions, reasons for inclusion, and requirements to support implementation activities. The implementation guidance is useful for defining policies and scope for an OT security program.

*NIST 800-82 and 800-160 are to be reviewed in full, rather than just as introductory guidance as recommended in Section 2.

Owner/Operator Has Implemented an IT/OT Cybersecurity Program

If companies have already implemented an IT/OT cybersecurity program, but would like to determine either the standard(s) to which they should certify their programs or best practices to which they should assess their programs, there are a number of factors that should be considered when choosing which standards and best practices to consider. These include, but are not limited to:

- Regulatory requirements
- Based in the U.S. or internationally
- Risk level
- Functions performed by the asset
- Extent of integration between IT/OT
- Level of IT/OT complexity
- Reliance on OT to perform safety-critical functions

The research team developed decision trees that present a series of yes/no questions related to these factors. Answering these simple questions in sequence will categorize an asset and identify all applicable (light-green cell and a gray circle) and recommended standards/best practices (bright-green cell and a white checkmark). Non-applicable references are noted with a gray cell. For the purpose of the annual report, we have included 1 (of 3) decision tree examples in Appendix C-3 of this report.

2.3.11. Regulatory Oversight

Based on the asset classes within the scope of the analysis, there are a number of Federal, international, and state/local agencies responsible for oversight of industry's safety and/or security programs. Table 8 lists the relevant Federal and international agencies and briefly describes their mission.

Table 8. Federal and International Regulatory Agencies

Agency	Mission
USCG	In the execution of its *Marine Safety* mission, the USCG provides clear and timely regulations, policy and direction to maritime stakeholders to achieve maritime safety, maritime security and environmental stewardship.
Bureau of Safety & Environmental Enforcement (BSEE)	BSEE is responsible for promoting safety, protecting the environment, and conserving resources offshore through regulatory oversight and enforcement.
DHS ISCD	DHS ISCD oversees the Chemical Facility Anti-Terrorism Standards (CFATS) program which identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce risks.
Department of Transportation (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA)	PHMSA's mission is to protect people and the environment by advancing the safe transportation of energy and other hazardous materials that are essential to our daily lives. To do this, the agency establishes national policy, sets and enforces standards, educates, and conducts research to prevent incidents.
Environmental Protection Agency (EPA)	The EPA's basic mission is to protect human health and the environment -- air, water, and land. EPA, state, local and tribal agencies work together to ensure compliance with environmental laws passed by Congress, state legislatures and tribal governments
IMO	The IMO is the United Nations' specialized agency responsible for improving maritime safety and preventing pollution from ships.
Occupational Safety & Health Administration (OSHA)	The OSHA's mission is to assure safe and healthful working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education and assistance.

In addition, there are numerous state and local agencies with oversight over select assets; and while not regulatory in nature, for DoD vessels and facilities, there are numerous internal standards and policy documents addressing cybersecurity and cybersafety issues. Figure 4 illustrates the regulatory oversight, both from a safety and security perspective, of many asset types that typically operate in the U.S. MTS.

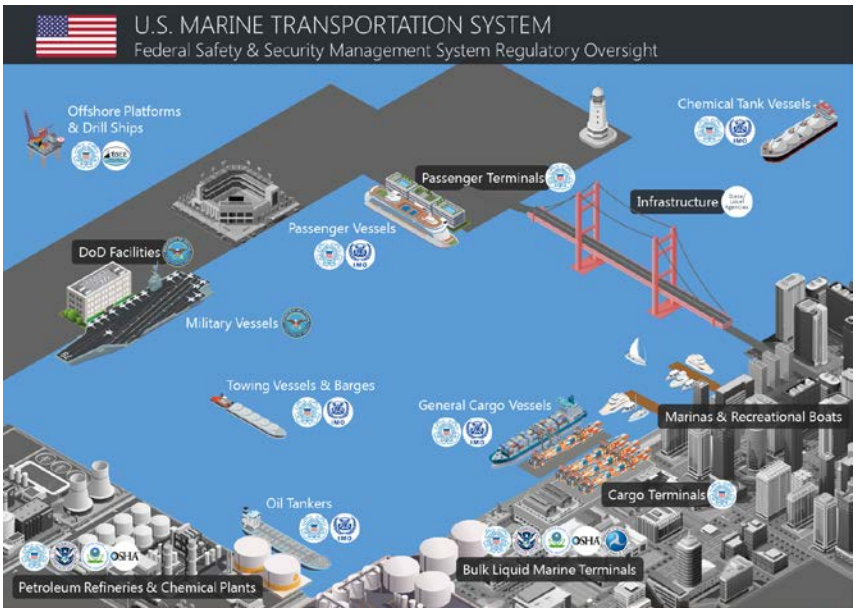


Figure 4. Regulatory Oversight for Common MTS Components

2.3.12. Security Management Systems

Table 9 summarizes each of the key Federal and international regulations and/or standards that collectively require security management systems for major assets that operate with the U.S. MTS. For the purpose of the annual report, we have included 1(of 5) Security Management Systems.

Table 9. Security Management System Regulations

33 CFR Subchapter H, Part 104 – Maritime Security: Vessels **Release Year:** 2003
Asset Applicability
Part 104 has provisions that applies to commercial vessels that operates in the U.S. MTS • Specific requirements for U.S. commercial vessels, including: passenger vessels, cargo vessels, tank ships, barges, towing vessels, and mobile offshore drilling units (MODUs) • Incorporates IMO's ISPS by reference to ensure that all foreign commercial comply with equivalent security requirements
Description
This regulation provides performance standards to assist vessel owners/operators with performing vessel security assessments (VSAs) and developing vessel security plans (VSPs) that comport with national maritime security initiatives. The regulations

identify 23 vessel security requirements spanning organizational requirements, personnel roles/responsibilities, training, drills, exercises, communications, recordkeeping, and a variety of security measure categories.
Cyber Commentary
Cyber considerations are not explicitly addressed in the CFR; however, many of the requirements are worded broadly and could be interpreted to include cybersecurity in addition to physical security. Requirements related to the following, are of specific interest: • §104.200 Owner or operator • §104.210 Company Security Officer (CSO) • §104.215 Vessel Security Officer (VSO) • §104.220 Company or vessel personnel with security duties • §104.225 Security training for all other vessel personnel • §104.230 Drill and exercise requirements • §104.260 Security systems and equipment maintenance • §104.270 Security measures for restricted areas • §104.275 Security measures for handling cargo • §104.280 Security measures for delivery of vessel stores and bunkers • §104.285 Security measures for monitoring • §104.290 Security incident procedures • §104.300 General • §104.305 VSA requirements • §104.405 Format of the VSP

Table 10 summarizes each of the key Federal and international regulations and/or standards that collectively require safety management systems for major assets that operate with the U.S. MTS.

Table 10. Safety Management System Regulations and Standards

SOLAS Chapter IX: International Safety Management (ISM) Code **Release Year:** 1994
Asset Applicability
Commercial ships on international voyages (including passenger ships, cargo ships, and MODUs) and the port facilities serving these ships
Description
The purpose of this Code is to provide an international standard for the safe management and operation of ships and for pollution prevention. The Code establishes safety-management objectives and requires a SMS to be established by "the Company", which is defined as the ship owner or any person, such as the manager or bareboat charterer, who has assumed responsibility for operating the ship. The Company is then required to establish and implement a policy for achieving these objectives. This includes providing the necessary resources and shore-

based support. Every company is expected "to designate a person or persons ashore having direct access to the highest level of management".
Cyber Commentary
Cyber considerations are not explicitly addressed in the Code; however, many of the requirements are worded broadly and could be interpreted to include cyber-related impacts to vessel safety. Specifically, requirements related to safety and environmental protection policy, designated persons, resources and personnel, shipboard operations, emergency preparedness, and maintenance of the ship and equipment

For the purpose of the annual report, we have included 1 (of 6) Safety Management Systems.

2.3.13. Framework for Points of Failure Detection Methodology

Over the past few years, the maritime industry has been increasingly engaged in cybersecurity implementation; however, the best practices are still being formed and many programs are not adequately focused on solid principles of design and implementation. Clear design concepts and effective tools that focus maritime cybersecurity efforts are needed. This section begins reducing cybersecurity implementation guidance confusion by establishing a framework for evaluating an asset's potential points of failure.

2.3.14. Background

There are a number of facets that make designing implementing robust cybersecurity programs for maritime companies and assets difficult. These include, but are not limited to:

Varying Levels of Automation. There are a myriad of industries and asset types operating within the U.S. maritime domain, and expectedly, these assets have varying levels of reliance on IT and OT systems, ranging from purely manual to highly automated. Some of the most highly automated assets include: offshore drill ships, MODUs, cruise ships, chemical plants, petroleum refineries, liquefied natural gas (LNG) facilities, LNG carriers, and container terminals. Other assets control operations through mostly manual processes, relying on simple, isolated OT systems, or in some cases antiquated analog control systems.

Asset Mobility and Connectivity. Maritime transportation assets are primarily focused on heavy mechanical vessels and offshore assets that are highly mobile and operate in remote environments. Even so, critical equipment systems on marine and offshore assets are increasingly connected. This reliance on highly connected software controls makes these systems vulnerable to cyber-related failures.

Dependence on Suppliers. As the number and sophistication of IT/OT systems have increased, companies have become increasingly dependent on equipment vendors to maintain and upgrade their systems. Maintenance and instrumentation departments often rely on vendor technicians to troubleshoot and fix OT issues. For the most highly automated assets, there is often integration among OT systems spanning multiple vendors, introducing the possibility for operational upsets as changes to one system can affect the performance of others.

Emerging Cybersecurity Culture. Cybersecurity is commonly viewed by the maritime industry as the domain of IT specialists who speak a specialized language and deal in obscure concepts. Further, the volume of cybersecurity-related reference materials is massive. Industry leaders in the cybersecurity domain are primarily business, financial, and IT-centric enterprises that project sophisticated, complex, and expensive solutions. The maritime industry is somewhat (understandably) confused about the applicability of such solutions to its cybersecurity needs, especially in the context of OT systems

Confusing or Non-applicable Cybersecurity Guidance. Constant media reports of cyber threats and incidents are troubling to maritime industry leaders and managers, but they often struggle to understand how the reported incidents and potential solutions might pertain to their business. Mounting incident information without pertinent, clarifying, and actionable knowledge can be more confusing than helpful. Even "guidance" provided for the maritime industry is often focused on problems and solutions that are not relevant to maritime OT systems. So, the maritime industry is being offered large amounts of information on how to improve cybersecurity that are not based on solid engineering fundamentals that enable development of a cybersecurity program based on the specific needs of an individual organization.

2.3.15. Engineering Principles

The maritime industry needs to understand cybersecurity can be implemented based on proven engineering principles. Software applications and computer technologies are often the targets of cyber attacks designed to degrade or compromise their functionality. Systems are designed for a specific set of functions; so, the research team developed a reference model based on common safety-critical functions performed by maritime assets.

Since the information management system is real, but mostly unseen, the research team coined the phrase *virtual asset* to represent the structure and behavior of the collection of systems on an asset. The virtual asset is the aggregation of the software applications and computerized technologies control mechanical systems that fulfill safety-critical functions. For an oil tanker, these might include ship handling activities (e.g., propulsion, navigation, ballast) and mission-oriented activities (e.g., cargo management). For the near future, human operators will interact with the virtual asset introducing variability to the system and the capability to handle exceptional events.

This virtual asset concept is important because it enables the establishment of dimensions that can be discussed in connection to cybersecurity implementations.
A basic engineering approach is decomposing complex systems into well-understood components that can be described and measured. The research team has decomposed the virtual asset into three components:

1. **Functions.** Software applications that control machines aboard the physical asset.
2. **Connections.** Nature and number of digital interfaces are measurable characteristics indicating cybersecurity complexity.
3. **Identities.** Endpoints or nodes (humans or machines) that send or receive data by means of the digital interfaces.

By observing the behaviors and interactions of a virtual asset's (1) functions, (2) connections, and (3) identities, a foundational understanding of cybersecurity requirements and points of failure is possible from an engineering perspective (Figure 5).

A fundamental cybersecurity concept is *trust*. The intent of a cybersecurity program is to establish trust with respect to functions, connections, and identities. If the behaviors of all three of the basic components of the virtual asset are trusted, then the asset is secure. If any behavior of one of the three components is not trusted, then the asset is not secure.

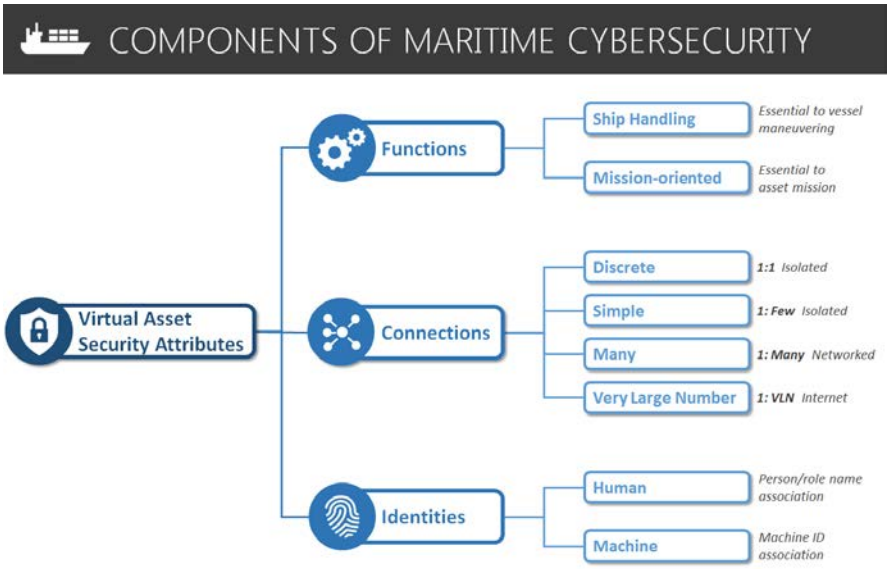


Figure 5. Components of Maritime Cybersecurity

Another basic engineering principle is experimental observation and measurement. With respect to cybersecurity, determining which things to measure may not be obvious, because the virtual asset can be somewhat abstract. But, when contemplated in terms of functions, connections, identities, business attributes, and documentation attributes, the measurement of a number of useful cybersecurity system characteristics emerges,

as does important understanding about the potential point of failure. The collection of useful data depends on (1) measuring the breadth and depth of the virtual asset and (2) subsequently collecting data concerning the attributes of functions, connections, and identities.

By describing the virtual asset, and subsequently collecting and measuring related data, it is possible and essential to impose risk-based standards into the design, implementation, and improvement of a cybersecurity system for maritime assets.

2.3.16. Framework

The research team developed the framework by identifying a simple set of virtual asset attributes that are essential to understanding potential points of failure. The sheer diversity of maritime asset types calls for a general use cybersecurity framework that can be easily tailored to be applied to any single asset instance. Using the framework to assess a given asset will provide useful information to assess its cybersecurity profile and focus subsequent assessments and improvement actions. The general framework is based on an understanding of the virtual asset's breadth and depth.

Virtual Asset Breadth is defined by the number of critical cyber-related functions on an asset. As a practical matter, these are commonly the functions that are critical for safety of people on the asset, the integrity of the asset itself, and/or the protection of the surrounding environment. To define the breadth, it is necessary to identify (inventory) each of the safety-critical functions on the asset. The framework defines two major categories for asset functions:

1. **Ship Handling** functions are for vessel assets only and address those functions required to ensure safe movement of the vessel and prevent collisions, allisions, groundings, etc. Common ship handling functions include: navigation, propulsion, ballast, power, and communication.
2. **Mission-oriented** functions are defined by the purpose or mission of the specific asset. If the asset is a cargo vessel, these functions will include cargo management and vapor control. For a drill ship, these functions will include drilling and well control.

Virtual Asset "Depth" is defined by complexity of the asset functions, business attributes, and the completeness of the system documentation. Depth is assessed by inventorying (1) the cyber complexity of the safety-critical functions, (2) the business constraints and capabilities of the enterprise, and (3) the availability of cybersecurity documentation that demonstrates the engineering rigor and execution within the enterprise. Further segmentation on the depth categories are:

1. **Cyber Complexity Attributes Inventory**
   - Functions: Criticality of functions to safe operation
   - Connections: Complexity of connections

- Identities: Accessing identities

2. **Business Attributes Inventory**
   - Regulatory imperatives
   - OT deployment strategy
   - Cybersecurity governance

3. **Cybersecurity Documentation Inventory**
   - Security responsibility evidence
   - Design knowledge evidence
   - Security control process evidence

2.3.17. Cyber Complexity

The research team developed a series of questions for each of the functions identified for the asset. The type of answer for each question is identified in parentheses at the end of the question. *Note: questions are worded so that affirmative responses for Yes/No questions indicate higher potential cybersecurity vulnerability.*

1. **This function is deployed on one or more assets within the enterprise (Number of Instances).** For each ship handling and mission-oriented function, indicate whether multiple instances of the function are installed at multiple assets or locations. This information is used to determine whether functions are copied exactly from location to location when designing protection systems. This can present opportunities for economy-of-scale protection or assessment considerations.

2. **This function is critical to safe operation (Yes/No).** Indicate whether degradation of performance or failure of the function can result in injury or loss of life to personnel, damage to or loss of the asset, and damage to the marine or surrounding environment.

3. **This function communicates using a well-understood connection type (Control Connection Type).** For each function, determine if the control system communicates by means of a discrete, simple, complex, or VLN connection.

   - **This function's control connection is "Discrete."** This type of connection may be characterized as a "1:1" connection in which the equipment is linked to its control connection only. This connection type communicates only with the equipment under its control, and is not connected to any other systems on the asset.
   - **This function's control connection is "Simple."** This type of connection may be characterized as a "1:Few" connection in which the equipment is linked to multiple other control connections directly and without a network.

- **This function's control connection is "Complex."** This type of connection may be characterized as a "1:Many" connection in which the equipment is linked to multiple on-asset control connections through a network.
- **This function's control connection is "VLN."** This type of connection may be characterized as a "1:VLN" in which the equipment is linked to the Internet, often by means of a network, and is therefore potentially connected to a VLN of off-asset nodes.

4. **This function is managed by the provider of the equipment and/or control system provider (Yes/No).** Indicate whether (1) the equipment and/or control system is managed as a service and (2) the service includes cybersecurity monitoring and protection.

5. **This function does not have supplier-provided control system documentation (Yes/No).** Indicate whether the equipment and control system are accompanied by a functional description document (FDD) that clearly explains the functionality of the equipment, diagrams the control system, describes its interfaces, defines its failure states, etc.

6. **This function's control system is protected by the system supplier's cybersecurity system (Yes/No).** Indicate whether the supplier of the control system has provided its own proprietary cybersecurity system with the control system, and if it is excluded from the widely installed security systems on the asset.

2.3.18. Business Attributes

The research team developed a series of Yes/No questions to be answered to describe the business attributes of the asset and enterprise. *Note: questions are worded so that affirmative responses indicate higher potential cybersecurity vulnerability.*

1. **The asset is not MTSA-regulated (Yes/No).** Indicate whether controls required by MTSA are in place on one or more assets within the enterprise, indicating full adherence to the requirements of that regulation.
2. **The asset is not registered with a classification society that has cybersecurity guidance (Yes/No).** Indicate whether classification society "rules" are implemented on the asset and may provide additional requirements for a cybersecurity implementation. *Note: this question does not apply to facilities.*
3. **Land-based IT or OT systems communicate to the asset's OT systems (Yes/No).** Indicate whether internal or 3rd-party land-based computerized systems communicate directly to a control system on the asset or to a network to which OT system or systems are connected.
4. **Some assets are identically equipped (Yes/No).** Indicate whether OT system designs (architectures) are duplicated (i.e., exact copies) within the fleet (clarification will be needed from the client), and may therefore offer opportunities for economy-of-scale with respect to design, implementation, maintenance, and assessment/notation.

5. **The company has not developed policy governing IT cybersecurity (Yes/No).** Indicate whether IT system security policies and procedures are documented, fully implemented, and available for review, indicating that the enterprise recognizes the importance of cybersecurity policies and procedures for business systems.
6. **The company has not developed policy governing OT cybersecurity (Yes/No).** Indicate whether OT system security policies and procedures are documented, fully implemented, and available for review, indicating that implementation of a fully capable OT cybersecurity program is planned, in progress, and may require only minimal additional assistance to complete.
7. **OT cybersecurity is provided by a 3rd-party supplier (Yes/No).** Indicate whether a cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protections, indicating that the cybersecurity implementation team and assessment team will have to support additional collaborations to perform activities; further, support from both internal purchasing and legal resources might be required for program implementation.

2.3.19. Cybersecurity Documentation Attributes

The research team developed a series of Yes/No questions to be answered to describe the cybersecurity documentation attributes of the asset and enterprise. *Note: questions are worded so that affirmative responses indicate higher potential cybersecurity vulnerability.*

1. **IT Cyber Security Office (CSO) responsibilities are not documented (Yes/No).** Indicate whether an office or named individual is responsible for security of IT systems. An internal authority indicates commitment to a culture of IT cybersecurity and provides an internal resource to support assessment activities.
2. **OT CSO responsibilities are not documented (Yes/No).** Indicate whether an office or named individual is responsible for security of OT systems. An internal authority indicates commitment to a culture of OT cybersecurity and provides an internal resource to support assessment activities.
3. **Incident Response Team (IRT) responsibilities are not documented (Yes/No).** Indicate whether an office or named individual is responsible for supervising the response to security incidents related to OT systems. A commitment to this function indicates that the enterprise is fully aware of the liabilities associated with a cyber incident and is organized for a rapid response and mitigation effort.
4. **An OT FDD has not been developed (Yes/No).** Indicate whether the OT systems being protected are inventoried and described in a client-generated, asset-specific design document, indicating that the enterprise understands that an engineering description of the functions requiring cyber protection is essential to the requirements development of a cybersecurity system and has invested in developing that description. The FDD also provides the foundation for an expeditious cybersecurity assessment or inspection by classification societies and regulators. See Appendix A for additional explanation of the OT Functional Description Document (OT-FDD).

5. **A compiled cybersecurity FDD is not available (Yes/No).** Indicate whether the cybersecurity systems providing protection are inventoried, described, and made available in a client-generated, asset-specific design document, indicating that the cybersecurity system is designed, implemented, maintained, and evolved as a rigorously designed and documented critical function and is subjected to rigorous change management control.
6. **Management of Change (MoC) documents are not available (Yes/No).** Indicate whether all changes to the OT and cybersecurity systems are rigorously controlled and governed by policy, procedures, and archived MoC documentation, indicating that the enterprise comprehends the evolving nature of cyber threats and the need to embrace and rigorously manage that evolution.
7. **Cybersecurity Training documents are not available (Yes/No).** Indicate whether home office and on-asset cybersecurity training is rigorously performed, managed, and governed by policy and procedure, indicating that the enterprise is embedding cybersecurity awareness and capabilities in the organization at all levels. Robust training practices also give indications of management commitment to do what is reasonable and prudent to protect lives, assets, and the environment from hazards potentially created by cybersecurity incidents.

Appendix C-4 presents an example of the point of failure detection framework worksheet tailored to the functions of a drill ship or MODU. The research team believes that this framework is useful because it provides a method for determining points of failure of an asset's cybersecurity based on unprotected functions, connections, and identities; where the notion of "point of failure" includes the system lifecycle process considerations to include agreement processes, an organization's enabling processes, technical management processes, and technical processes.[6] This approach is extensible for the development of a qualitative or qualitative measure of an asset's cybersecurity profile. This measure (1) can be derived from the responses to the statements posed in the virtual vessel breadth and depth assessment and (2) could be associated with C2M2 Maturity Indicator Levels (MILs) to characterize the maturity of the asset's cybersecurity:

Level 3: Managed
Level 2: Performed
Level 1: Initiated
Level 0: Not Performed

2.4. VTS Radar

2.4.1. Introduction

The US Coast Guard uses a Vessel Traffic Service system to collect, process, and disseminate information on the marine operating environment and maritime vessel traffic in major U.S. ports and waterways. The PAWSS (Ports And Waterways Safety System)

[6] NIST Draft Special Publication 800-160, 2016

VTS mission is to monitor and assess vessel movements within a VTS Area, exchange vessel movement data with vessel and shore-based personnel, and provide advisories to vessel masters.

The VTS system at each port has a Vessel Traffic Center that receives vessel movement data from the Automatic Identification System (AIS), surveillance sensors, other sources, or directly from vessels. AIS technology relies upon global navigational positioning systems (GPS), navigation sensors, and digital communication equipment operating according to standardized protocols (AIS transponders) that permit the exchange of navigation information between vessels and shore-side vessel traffic centers. AIS transponders can broadcast vessel information such as name or call sign, dimensions, type, GPS position, course, speed, and navigation status.

While AIS is helpful, not all vessels are required to use AIS (only certain vessels that fall under certain categories for gross tonnage, passenger capacity, length, and function are required to carry and use AIS). Also, the majority of currently installed radars detect vessels with a minimum size where smaller vessels and other objects that have too small of a Radar Cross Section are not seen in the background of clutter. Therefore, a means is needed to detect these small and large vessel targets that are either not required to carry AIS or not cooperative (i.e., they do not comply with AIS required use or spoof AIS information).

2.4.2. Project Objectives

As a first step, this project aims at conducting a market survey to learn about commercially available solutions that have been developed to address this. In particular, we will research and document open source information for commercial solutions that provide clutter suppression methods to improve radar performance. We will also survey standards and integration patterns that are applicable in this area.

Once the commercial solutions are understood, we will examine radar raw data that contains all the detected information, including small targets and unwanted clutter.

The objective of this research is to help DHS stakeholders in their operational missions to identify suspicious small vessels that may be present in a harbor or port. It addresses one of the Secure Borders Integrated Product Team (IPT) gaps (see https://www.dhs.gov/science-and-technology/ipt) as well as questions provided in the Center FOA. These questions are:

- What existing technologies can be applied to effectively improve surveillance, detection, classification, and identification of vessels, suspicious materials, and persons in the maritime domain both on and below the water?

- What new technologies, including technologies combined with new non-technological inspection methods and tools, can effectively improve a user's ability to screen, detect, and mitigate threats?

The USCG has invested in many VTS/PAWSS installations around the US ports. Although their objective is to detect large vessels using Terma based radars, the raw radar data could contain detections of small vessels as well. The objectives of this proposal is to:

1. Perform a market survey for software standards, integration patterns and security requirements that are applicable in this area;
2. Investigate various industry standards for exchanging real-time radar data such as NMEA OneNet and Asterix;
3. Investigate and document existing commercially viable systems for clutter suppression methods for improving radar performance through open source information;
4. Investigation of new algorithms and known signal processing algorithms and sea clutter suppression methods that can provide longer range of small boat detection.

2.4.3. Milestones

This project started in Year 3, but the scope was modified after the start date. Therefore, the project results with the following milestones will be reported in Year 4's annual report.

Milestone	Description	Outcomes
1	Kick-off meeting with key stakeholders from DHS, CBP, and USCG.	Meeting notes
2	Survey of software standards, integration patterns, and security requirements	Draft 1 Summary Report
3	Investigation of the application of NMEA OneNet, Asterix formats, and other National Marine Electronics Association (NMEA) communications protocols for organizing the radar network and for data fusion with information from other sensors (like AIS and Maritime CCTV surveillance).	Draft 1 Summary Report
4	Investigation of existing commercially viable systems for clutter suppression methods for improving radar performance through open source information	Draft 2 Summary Report
5	Investigation of new algorithms and known signal processing algorithms and sea clutter suppression methods that can provide longer range of small boat detection.	Draft 2 Summary Report

6	Documentation of all findings	Final Summary Report

3. Education and Outreach

3.1. Overview

MSC has continued to build upon the robust portfolio of educational programs that it developed to enhance the technical skills and leadership capabilities of current and prospective maritime and homeland security practitioners. The Center's educational programs leverage the subject matter expertise and research capabilities of its academic partners to provide multidisciplinary hands-on learning opportunities and degree granting programs for a broad audience of students, professionals, stakeholders, and the general public. During Year 3, MSC offered the following homeland security-focused professional development and college-level educational programs:

- Maritime Incident Discussion-based Tabletop Exercises
- Summer Research Institute (8th annual)
- Maritime Security Master's and Doctoral Fellowship Programs
- Maritime Security Seminar Series
- USCG Auxiliary Program

MSC's educational programs are offered in collaboration with the Center's network of stakeholders. MSC stakeholders include the U.S. Coast Guard, Customs and Border Protection, New York Police Department – Counterterrorism Division (NYPD-CTD), National Urban Security Technology Laboratory (NUSTL), Port Authority of New York and New Jersey (PANYNJ), New Jersey Office of Homeland Security and Preparedness (NJOHSP), and the Sector New York Area Maritime Security Committee (AMSC), to name a few. These stakeholders have contributed to the Center's educational programs by hosting field-visits, providing feedback on course content and curriculum, input on student research projects, training opportunities, and field-based internships and employment opportunities.

This section of the report provides a summary of the Center's education milestones, followed by a detailed account of the MSC's educational programs and outreach activities during Year 3.

3.2. Summary of Education Milestones

3.2.1. Maritime Incident Discussion-based Tabletop Exercises

In Year 3, MSC in conjunction with SDMI at Louisiana State University (LSU) assisted in the development and delivery of three Maritime Cybersecurity tabletop exercises for the USCG Sector New York AMSC Cybersecurity Sub-Committee. The exercises involved

hypothetical cyber threat scenarios impacting the operations of container terminals, passenger ferries, and oil and gas terminal operators in the Port of New York and New Jersey.
Leveraging the materials created for the AMSC Cybersecurity tabletop series, as well as those created during Year 2 (e.g. Active Shooter exercises for the Port of New Orleans), the Center created a portfolio of Exercise Development Kits that can be used by the maritime and port community to exercise their own preparedness and response capabilities. The Exercise Development Kits can be reviewed and downloaded from the Center's website at: https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/tabletop-exercise-development-kits

3.2.2. Maritime Seminar Series

MSC hosted two guest speakers in the Center's Maritime Seminar Series during Year 3. The guest speakers included a research scientist in Entomology from Stevens Institute of Technology and a Security and Global Studies instructor from the American Military University. The seminars explored issues regarding the impacts of invasive species on the U.S. agricultural system, and ethical and legal considerations as they relate to the use of cyber intelligence and counterintelligence. Seminar feedback and recommendations for future seminar topics were obtained through participant surveys. A decision to discontinue the Maritime Seminar Series was made by the Center's biennial review committee in March 2017.

3.2.3. 2017 Summer Research Institute

MSC successfully delivered its 8th annual Summer Research Institute (SRI), from June 5 to July 28, 2017 on the campus of the Stevens Institute of Technology in Hoboken, NJ. Twenty-two students engaged in the eight-week intensive program, representing seven U.S. universities, including students from two Minority Serving Institutions. The average GPA for the student group was a 3.7 out of a 4.0. The students engaged in a minimum of six faculty and guest lectures and attended three field-visits and multiple experiments in conjunction with MSC researchers and stakeholders. The SRI student participants were organized into four research teams, each producing a final team report, research posters and final oral presentations.

3.2.4. Doctoral Fellowships

Maritime Security Doctoral Fellowship

Mr. Alex Pollara completed his third and final year in the Maritime Security Doctoral Fellowship program. Throughout the 2016/2017 academic year, he published two peer-reviewed journal papers and presented conference papers at four conferences. He has completed his degree requirements and is scheduled to defend his dissertation in August 2017.

Mechanical Engineering and Homeland Security Doctoral Fellow

Mr. John Martin completed his second year in the Mechanical Engineering & Homeland Security Doctoral Fellowship. During the 2016/2017 academic year, he completed 24 additional credits towards his doctoral degree program and submitted two conference papers for consideration.

3.2.5. Undergraduate and Graduate-level Research Assistantships

MSC supported two students in Research Assistantships at Stevens Institute of Technology during Year 3. The undergraduate and graduate-level students each conducted research in support of the Center's projects in the areas of Mobile Maritime Domain Awareness and Unmanned Systems, as well as their own academic program research in the areas of AIS spoofing and fraud, and acoustic buoys. The students were each enrolled full-time and maintained above a 3.30 cumulative GPA.

During Year 3, Graduate Research Assistant, Blaise Linn, completed his degree requirements to receive his Master of Science degree in Maritime Systems at Stevens Institute, and has been retained by the university for the duration of the summer months (June – August) to provide continued research support and assistance to the MSC Summer Research Institute.

3.2.6. Maritime Systems Master's Degree (CDG) Fellowship Program

In Year 3, the student in the DHS CDG funded Maritime Systems fellowship program successfully completed his degree requirements to receive a Master's degree in Maritime Systems with a Graduate Certificate in Maritime Security. He is the ninth student to complete the Center's two-year fellowship program. He recently accepted a short-term position with Stevens Institute of Technology serving as a Research Assistant while continuing to pursue career opportunities in the Homeland Security enterprise.

In an effort to track the career trajectories of the Center's fellowship program alumni, the Center prepared and distributed a post-program survey to track the homeland security employment and career activities of students following the completion of their degree programs. Survey responses reported that all of the Fellowship students had successfully met their one year post-program HS employment, and all but one continues to work in support of the Federal government and its component agencies. (e.g., DHS, DOE, and DOD).

3.2.7. MSI Outreach and Engagement in Research

MSC in conjunction with a faculty and student research team from the University of Texas Rio Grande Valley (UTRGV) were selected to participate in the DHS OUP Minority Serving Institutions (MSI) Summer Research Team Program (SRTP). The ten-week summer research program was held on-campus at Stevens Institute of Technology and included research into the uses of virtual reality (VR) applications to support homeland security training and field-based operations.

3.2.8. USCG Auxiliary Program

Due to membership attrition and changes in mentorship support by the USCG Auxiliary Flotilla 21, Stevens did not hold regularly scheduled meetings and activities during Year 3. Through the 2016/2017 academic year, MSC pursued alternative opportunities for Stevens faculty and student Auxiliary members to attend meetings and activities off-campus at other local Flotilla locations (e.g. Secaucus, NJ and Lower Manhattan). A decision to discontinue the campus-based USCG Auxiliary program was made by the review committee during the Center's biennial review in March 2017.

The remaining section of the education annual report includes details regarding each of the programs summarized above.

3.3. Professional Development Programs

3.3.1. Maritime Incident Discussion-based Tabletop Exercises

Milestones	Performance Metrics	Status / Discussion
1. Develop Advisory Group to provide input and guidance in the development of scenarios and the exercise resource portal.	Advisory committee established to include representatives from a minimum of two port facilities. Advisory members will also include a representative(s) from the USCG, and other state and local port partner organizations.	Completed: An advisory committee was formed to include representatives from the MPS ISAO, Port of New Orleans, Port of South Louisiana, Louisiana Fusion Center, Louisiana National Guard, USCG, and LSU
2. Develop exercise scenario tools/templates for Active Shooter and Cyber Security Attack exercises.	The exercise resource portal will be developed to include a minimum of two Exercise Development Kits. .	Completed: Tabletop exercise resource materials were developed, to include exercise templates and facilitator guides for a series of four Active Shooter and one Cyber Attack scenarios.
3. Identify new port partners to collaborate with and to develop a new discussion-based exercise.	MSC identifies a minimum of two new port partners to assist and support in their development of customized exercises.	Completed: New partnerships were formed with the Gulf of Mexico AMSC and SDMI assisted in the development and delivery of a tailored Cybersecurity tabletop exercise. SDMI also collaborated with the Port of South Louisiana, the largest tonnage port in the U.S. to assist in identifying new

		scenarios for the port to exercise in FY-18.
4. Develop online/web-based portal to host Exercise Development Kits.		Completed: The Active Shooter and Cyber Attack Exercise Development Kits have been made available and download on the MSC website.

During Year 3, MSC in conjunction with its academic partners from Stephenson Disaster Management Institute (SDMI) at Louisiana State University (LSU) continued to expand upon its outreach to the maritime and port community and develop and deliver relevant maritime incident discussion-based tabletop exercises tailored to enhance the preparedness and response capabilities of maritime and port facility operators.

As part of its efforts, the MSC/SDMI team assisted in the development and delivery of three Cybersecurity tabletop exercises in conjunction with the USCG Sector New York Area Maritime Security Committee Cybersecurity Sub-Committee and the USCG Exercise Support Team. The three exercises involved hypothetical cyber threat scenarios impacting the operations of container terminals, passenger ferries, and oil and gas terminal operators in the Port of New York and New Jersey.

The exercises were designed and intended to raise the cybersecurity awareness in the Port of NY/NJ, inspire port partner collaboration and information sharing, and to enhance the cybersecurity posture of the NY/NJ port enterprise. Held August 9-11, 2017, the tabletop exercises included participants from the following organizations:

- **Container Terminals**: Maher Terminal, APM Terminal, Port Authority Container Terminal, Red Hook Terminal and Global New York Container Terminal
- **Oil and Gas Operators:** Phillips 66, IMTT Bayonne, Kinder Morgan, Kuehne and Sunoco Partners
- **Ferry Operators:** Waterways and Sea Streak

An internal after-action report was prepared by the Sector NY and outcomes from the exercises were discussed at a September 2017 members at large meeting. The MSC/SDMI team was recognized for their contributions in developing and facilitating the exercises in a letter of citation from Captain Michael Day, Commander Sector NY.

New Port Partners

SDMI was invited to participate in the Gulf of Mexico Area Maritime Security Committee to help develop a comprehensive Gulf-wide cyber attack table top exercise. SDMI was part of the Exercise Support Team which was led by the NCCIC's Cyber Exercise Team and specifically participated in the development of the scenario that was used to build the exercise. In addition, SDMI was asked to take the lead and provide training on cybersecurity to the AMSC exercise participants. The training resulted in three modules: Cybersecurity for Information Technology Systems, Cybersecurity for Operational Technology Systems, and Cyber Capabilities (Federal, State and Local) to support the Maritime Community during a major attack. More than 60 people participated in the training. The exercise is scheduled to take place on August 9, 2017 at the New Orleans Office of the Bureau of Safety and Environmental Enforcement and includes over 150 participants from Texas, Louisiana, Alabama, and Florida.

SDMI has also developed a new partnership with the Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO), which has a nationwide reach. SDMI was invited to brief cyber threats and cyber risk management at its first annual cyber symposium. SDMI and MPS-ISAO are partnering to provide additional capabilities to the port community on cybersecurity.

Exercise Development Kits

Leveraging the materials developed for the AMSC Cybersecurity tabletop series, as well as those created during Year 2 (e.g. Active Shooter exercises for the Port of New Orleans), SDMI convened an Advisory Group of maritime security practitioners, exercise designers, and port operators to provide input and guidance into the development of resource materials and maritime incident focused Exercise Development Kits.

The exercise development advisory group includes the following representatives:

- Mr. Paco Capello, Chief Information Security Officer, LSU Transformational Technologies and Cyber Research Center.
- Mr. Roy Ford, Port Security Specialist, Sector New Orleans
- MAJ.Neal Fudge, Operations Officer, Louisiana National Guard, Certified Exercise Practitioner
- Mr. Devin King, Formerly with LA-SAFE (Fusion Center) and now with LSU Transformational Technologies and Cyber Research Center
- Mr. Lester Millet, Port of South Louisiana, Safety Agency Risk Manager / FSO Working Group Chairman, President of Infraguard Louisiana
- LT Michael Sawyer, Port of New Orleans
- Ms. Lauren Stevens, Associate Director of Disaster Management Programs, LSU-SDMI, Certified Exercise Practitioner

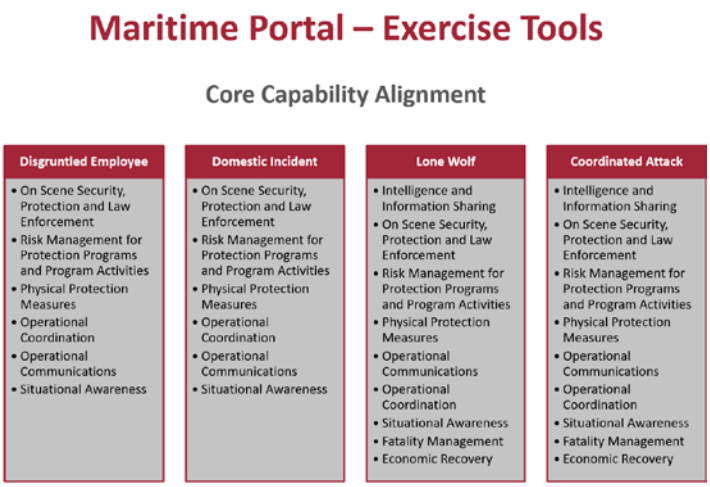


Figure 1. MSC Exercise Development Kits are designed to test core capabilities.

Exercise Development Resource Materials

Active Shooter Exercise Development Kits

With the intent to provide the exercise design team with a full range of active shooter based scenarios, this exercise design series consists of four different aspects of an active shooter scenario. The four modules are based on the following potential scenarios: 1) An active shooter that involves a disgruntled employee; 2) an active shooter that involves a domestic dispute in or near a cruise terminal; 3) a lone wolf terrorist attack at an active cruise terminal; 4) a complex coordinated terrorist attack at a cruise terminal.

These modules are meant to be used individually based on the current capabilities of a port system, or to be conducted as two or more exercises that allow a port system to establish a foundation on their overall response capabilities, with the ability to add more complexity and challenges to a significantly more difficult scenario.

Cybersecurity Exercise Development Kit

Based on the reach and complexity of a potential cyber attack throughout the entire maritime sector, the exercise development kit is designed to allow an exercise support team to integrate cyber attacks on key systems that are commonly found in port facilities. The intent is to allow the team to introduce a variety of cyber based injects to meet specific requirements and introduce attacks on multiple facilities or attacks throughout the entire port system. By developing injects for critical systems, the design team has the flexibility to create a wide variety of cyber attacks based on the goals and objectives of the exercise. In addition, the multiple injects allow for a wide array of sophistication based on the skill level of the actual exercise players.

Each of the five Exercise Kits contain the following components:

1) **List of Potential Players** – to help exercise support teams to identify the appropriate players for each of the exercise scenarios, a comprehensive list of agencies representing entities that have a role or are affected by either an active shooter or cyber attack is provided. The lists are meant to serves as a guide on potential agencies that would have an important capability / responsibility in the identified scenario.

2) **Core Capability Alignment** – To facilitate alignment of core capabilities with the exercise objectives, a list of core capabilities that are aligned to an active shooter and cyber attack within the port system are included in the kit.

3) **Recommended Objectives** – For each of the relevant core capabilities, the exercise design kit provides potential / sample objectives that can be leveraged for the actual exercise. These objectives are intentionally written generically and not specific to any particular participant or process being evaluated in an exercise.

4) **Scenario Builder** – The scenario builder provides multiple injects for each of the modules within the exercises. The multiple injects allow the exercise design team to take different routes for a cyber attack or active shooter event while increasing the overall level of complexity and range of the event. The injects can be combined or altered to fit specific industries within the port system.

5) **Facilitator Guide** – The facilitator guide identifies questions that a facilitator can use during the actual exercise. The list of questions represents a significant starting point that can be leveraged to help in the process of identifying and completing the desired questions that will ultimately be used during the execution of the exercise.

The Exercise Development Kits have been made available for review and download on the MSC website at: *https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/tabletop-exercise-development-kits*

3.3.2. Maritime Systems Seminar Series

Milestones	Performance Metrics	Status/Discussion
Delivery of maritime systems/homeland security focused seminars. Year 3 – 7/1/16 – 6/30/17.	-MSC will host six seminars during Year 3. -A survey will be used to assess the quality of the presentation, the relevance of the topic and to gather feedback for future seminars. -Webinars/Seminars will be made available to the public on the Center's website -Speakers will include MSC researchers and guest speakers from the homeland security domain.	Incomplete: The Center hosted two seminars during Year 3. A decision to discontinue the Seminar Series was made by the Review Committee during the Center's biennial review process. The Center therefore did not meet the stated milestone of six seminars. Completed: A survey was created and utilized to assess the two seminars and to gather feedback for future talks.

MSC with the support of other departments at Stevens Institute of Technology co-hosted two guest speakers in the Maritime Systems Seminar Series. The Year 3 seminar series included lectures by Dr. Helen Hull-Sanders, Stevens Institute and Edward Martinez, from the American Military University. The seminar series is designed to engage a broad audience of faculty, students, industry and government stakeholders, and the general public in relevant and timely topics in the maritime and homeland security domain. Some of this year's seminar participants included representatives from the U.S. Department of Agriculture, Rutgers University, and faculty members, students and administrators from Stevens Institute of Technology. The seminar series is delivered on-campus at Stevens Institute. Feedback from the seminars was gathered in the form of a survey distributed to participants who physically attended the seminar. Completed surveys demonstrated that the majority of participants attended the seminars from the Stevens community of faculty, staff and students, and that the seminars were attended out of personal interest and relevance to the attendee's job/academic program.

Following the Center's biennial review a decision was made by the review committee to discontinue the Seminar Series program. Therefore, no additional seminars were organized or held as part of this program for the remainder of Year 3. The seminars delivered during this reporting period are outlined in Table 1 below.

Table 1. Maritime Systems Seminar Series

Faculty/Guest Lecturer	Seminar	Date

Edward Martinez, American Military University	*Cybersecurity Policy and Ethics*	10.21.2016
Helen Hull-Sanders, Stevens Institute of Technology	*Crossing Borders - Invasive beetles find new homes and threaten mass deforestation in the U.S.*	10.06.2016

3.4. College-level experiential learning and research-based programs

3.4.1. The 2017 Summer Research Institute

Milestones	Performance Metrics	Status/Discussion
1. Featured lectures by MSC researchers and invited guests. (Weeks One – Eight) (6/5/17 – 7/28/17)	-A minimum of two homeland security/maritime industry guest speakers will be hosted during the summer research program. -A minimum of six faculty lectures will be provided during the eight-week program. -The quality of and knowledge learned from the lectures will be assessed through a post- program student survey.	Completed: Three guest speakers were hosted during the 2016 SRI. Eight faculty lectures were held during the first week of the SRI, with additional lectures held throughout the program. A post-program survey was distributed to the SRI student participants.
2. Field-visits and field-based activities. (Weeks One – Seven) (6/5/17 – 7/21/17)	-SRI students will engage in a minimum of two field-visits per summer research program. -MSC will facilitate a minimum of one field-based activity (meeting with stakeholders, research experiments/deployments, attendance at a workshop) during the program. -The impacts of the field-visits and field-based activities on student professional development and networking skills will be assessed through a post-program student survey.	Completed: Three field-visits were completed this summer. (CBP, Sector Long Island Sound and NY Waterways/Staten Island Ferry. Completed: Students participated in multiple field-based experiments, including deployment of an ROV in the Hudson River, ice fracturing experiments (125) in Stevens Anechoic Chamber and stability testing of a

		USV in Stevens aquatic center. Completed: A student survey was administered and completed by 20 of the 22 participants.
3. Diversity of student participants. (6/5/16 – 7/28/17)	-Diversity will be measured according to the range of engineering and science majors represented in the program. A minimum of four different disciplines will be represented per SRI program. - Student diversity will be measured by the percentage of women and minority students participating in the program each summer. A diverse student population will include a minimum of 50% women and/or minority students.	Completed: Student academic disciplines included 10 unique majors. Incomplete: Student demographics included 36% underrepresented students (women and minority students), less than the desired 50%.
4. Research Reports, Presentations and Posters. (Week Eight) (7/24/16 – 7/28/17)	-A minimum of two student research team reports will be prepared at the end of each SRI program. -A minimum of two student research team posters will be prepared at the end of each SRI program. -Students will engage in weekly status update presentations during weeks three – seven. -Stakeholder engagement will be assessed by representation of MSC stakeholders attending the final student team presentations. -Quality of SRI research outcomes will be assessed by MSC research mentor feedback and the number of projects selected for presentation at conferences and/or for publication. -Program impacts, e.g., professional development, technical skills learned, student interest in advanced academic study or careers in homeland security will be assessed by a post-program student survey.	Completed: Four student research reports were completed. The teams also prepared final presentation slides and three completed research posters. One team has prepared a journal abstract and plans to submit their research report for publication. SRI survey showed that students significantly improved their skills in several skill areas. 95% of the students reported that the SRI enhanced their interest in careers in HS.

5. Post-Program and SRI alumni survey. Post-program surveys to be conducted (Week Eight) (7/24/17 – 7/28/17)	-A minimum of one student survey will be conducted at the end of each summer research program. The survey will be used to measure the strengths and weakness of the program, the program's impacts on student interest and skills development, and to gather feedback to enhance the future delivery of the program.	Completed: A student survey was completed by the program participants and assessed by the MSC.

MSC held its 8th Annual Summer Research Institute from June 5 – July 28, 2017, at the Stevens Institute of Technology campus in Hoboken, NJ. Since the Summer Research Institute's inception in 2010, 138 students have conducted research in conjunction with MSC research PIs, stakeholders and Stevens' faculty members. Each year, the Center identifies a set of student research projects based on conversations and interactions with its stakeholder and takes into consideration the Center's ongoing and emerging areas of research. The SRI student research projects are purposely designed to expose students to critical issues in the maritime domain and to challenge them to find innovative and technological approaches to address them.

Figure 1. SRI 2017 Program Brochure

In 2017, the MSC hosted 22 student participants representing the following seven universities: Elizabeth City State University, Northeastern University, Stevens Institute of Technology, SUNY Maritime, University of Alabama-Huntsville, University of Alaska – Anchorage (UAA), and the University of Texas Rio Grande Valley. 82% of the student participants were undergraduates, and 36% of students were from underrepresented communities (e.g. women and minority students).

To support student participation in the 2017 summer research program (e.g., housing, stipend and travel), the Center leveraged existing Stevens Institute of Technology scholarship programs and those of its academic partners to recruit students who could attend the summer research program fully-funded through external funding sources. Out of the 22 program participants, 17 students attended the program leveraging funding from external sources including; Stevens Institute of Technology's Pinnacle Scholars Program (11), the Arctic Domain Awareness Center (ADAC) Fellows Program (2), the MSI Summer Research Team Program (2), and the NSF Maritime Cybersecurity project (2). 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 2 below shows a picture of the 2017 SRI participants on the first day of their program and Table 2 identifies the participants and the funding sources leveraged to support their participation.

Figure 2. SRI 2017 student participants.

Table 2. SRI 2017 Student Participants

University	Student	Major & Degree Status	Funding Source
Elizabeth City State University	Daniel Odell	Computer Science/Undergrad.	MSC
Northeastern University	Khiana Rogers	Civil Engineering	MSC

Stevens Institute of Technology	Michael Alecci Nicholas Duca Mathew Green Trevor Hinds Jared Hobbie Catherine Javadian Victoria Kapp Vincent Lee James Lyon Stephen Opet Anthony Orrico Gabrielle Padriga Max Panoff	Mechanical Eng./Undergrad. Finance/Undergrad. Naval Eng./Undergrad. Mechanical Eng./Undergrad. Cybersecurity/Undergrad. Cybersecurity/ Undergrad Mechanical Eng./Undergrad Comp. Science/Undergrad Chemical Eng./Undergrad Electrical Eng./Undergrad Computer Eng./Undergrad Comp. Science/Undergrad Electrical Eng./Undergrad	Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar NSF MSC Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar
SUNY Maritime	James Fredericks	Marine Operations	MSC
University of Texas Rio Grande Valley	Victor Carreon Juan Elizondo	Mechanical Engineering/Graduate Manufacturing & Industrial Engineering	MSI SRTP MSI SRTP
University of Alabama – Huntsville	Jennifer Li	Computer Science/Cybersecurity Graduate	NSF
Univ. of Alaska – Anchorage	Matthew Alrichs Kyle Alvarado James Matthews	Civil Eng./Graduate Mechanical Eng./Undergrad Civil Eng./Undergrad	ADAC ADAC MSC

3.4.2. Student Qualifications and Documentation

Participation in the Summer Research Institute 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 (Master's and PhD) students are required to have a GPA of 3.5 or better. This past summer's participants were required to complete an online application form, write a personal statement of interest, submit letters of recommendation and transcripts upon request. In accordance with Stevens policy, visiting SRI students were also required to demonstrate proof of health insurance and submit immunization records to Stevens Health Center prior to attending the program.

3.4.3. SRI Summer Research Stipends and Housing

MSC funded students (5) received summer stipends of $4,000 and were provided with accommodations on campus in the Stevens dormitory housing. Travel reimbursements up to $1,000 were also made available for transportation to and from the start and end of the program for students residing outside the state of New Jersey.

3.4.4. SRI Program Administration

The 8th annual SRI continued to be organized and coordinated by MSC Director of Education, Beth Austin-DeFares, in conjunction with Dr. Barry Bunin (Director, Stevens Institute of Technology Maritime Security Program). Ms. Austin-DeFares served as the primary program facilitator, while Dr. Bunin participated as the lead faculty facilitator and curriculum developer. Dr. Bunin also provided the day-to-day SRI student team mentorship, along with other MSC research PIs and Stevens faculty. In addition, Dr. Bunin served as the overall technical lead on the SRI projects and provided assistance to students in both theoretical and practical implementation of the projects. The SRI student team mentorship was provided by MSC research PIs and Stevens faculty including Dr. Brendan Englot (Assistant Professor, Mechanical Engineering), Dr. M.G. Prasad (Professor, Mechanical Engineering), Chen Zhao (Doctoral Candidate, Mechanical Engineering, Dr. Thomas Lechler (Assistant Professor, Business), Dr. Susanne Wetzel (Assistant Professor, Cybersecurity) and by MSC Research Assistant's Blaise Linn and Dmitriy Savinskiy.

3.4.5. SRI Program Format and Curriculum

WEEK ONE	JUNE 5 (Monday)	JUNE 6 (Tuesday)	JUNE 7 (Wednesday)	JUNE 8 (Thursday)	JUNE 9 (Friday)
	Program Starts at 2:00 PM **2:00pm Welcome – B. DeFares** **2:15pm Student Introductions** **2:45pm Mentor Introductions** **3:00pm break** **3:10pm Project Overviews – Discussion of Projects (5-10 mins. each)** **Virtual Reality – Blaise Linn** **Arctic Acoustics – Barry Bunin** **ROVs in Maritime and Port Security- Brendan Englot** **3.50pm Discussion - Team Assignments** **4:00pm – MSL Overview – B. Bunin/Dimitriy Savinskiy** **4:20pm –Student Guest ID's and Campus Tour (non-Stevens students)**	9:00am Intro to Marine Transportation System (MTS) Expansion of Global Trade since WWII – T. Wakeman	9:00am Development of Containers & Intermodalism Intro to Safety & Security in Ports – T. Wakeman	9:00am Observations Report-out and Discussion – T. Wakeman 11am Oceanography & Estuaries – T. Wakeman	9:00am Port Competition Presentations - Faculty
		Lunch	Lunch	Lunch	Lunch
		2pm - Guest Speaker Mr. Dana Goward, USCG SES (ret.) – Discussion on GPS Vulnerabilities 3pm History of Ships, Harbors/Ports, and Cargo Terminals – T. Wakeman	1pm Observations, Analysis and Threat Assessments **Field Visit – to Staten Island Ferry via Hoboken Ferry**	1pm Maritime Business "It's about the money!" – T. Wakeman	1pm **Student research team meetings with Mentors**

Figure 3. Schedule for Week One of the 2017 SRI.

The eight-week program includes a balance of in-class lectures, student team research projects, professional development activities, and several field-based learning opportunities. A formal orientation to the 2017 SRI was conducted during the first week of the program (June 5-9), however, a series of pre-reading assignments were sent to students the week of May 29, 2017, in preparation for the start of the program.

Dr. Thomas Wakeman, Director Maritime Systems Program at Stevens Institute, provided a sequence of introductory lectures tailored to immerse students in a comprehensive overview of the Maritime Transportation System (MTS). The lectures include talks on maritime security policies, maritime industry and government stakeholders, and port facility infrastructure and operations. With the exception of the Maritime Cybersecurity team who were organized through a Stevens-based NSF research project, the SRI student participants were also assigned into one of the following three projects:

- Remotely Operated Vehicle (ROV) and Unmanned Surface Vehicle (USV) Cooperation in Maritime and Port Environments
- Arctic Acoustics – Detecting and Localizing Changes in Ice Cover
- Virtual Reality (VR) Applications for Enhanced Maritime and Port Security

The fourth project, Maritime Cybersecurity – Data Flows in the Maritime Transportation System was developed as part of an NSF funded research project. MSC's director of education is a co-PI for the NSF project and included the Summer Research Institute into the project proposal. The students assigned to the SRI Maritime Cybersecurity project, were selected according to their participation in a Stevens NSF-funded Cybersecurity Scholars for Service program.

Starting Week Two, the program format shifted from time spent in the classroom to time spent engaging in team research projects, field-based visits and experiments, and meetings with maritime and homeland security practitioners. During the next five-week period, the student teams also began to provide status updates on their research in the form of weekly presentations. Each team was responsible for providing a fifteen to twenty-minute presentation discussing their research, field-based activities, and challenges and progress in their work. MSC hosted guest speakers from the Resilient Navigation and Timing Foundation, the U.S. Coast Guard Research and Development Center, and the NYPD-Counterterrorism Division during weeks one and two, and facilitated field-visits to Customs and Border Protection Field Operations at Port NY/NJ, Sector Long Island Sound in New Haven, CT, and security observations on the NY Waterways and Staten Island Ferries. Details regarding guest speakers and field-visits are provided later in this report.

In Week Seven, the student teams began to synthesize their research and started to compile their final team research reports with the support of their faculty mentors. In Week Eight, the last week of the summer research program, students submitted their final reports and provided team presentations to an audience of MSC researchers and administrators, and representatives from DHS and the Port Authority of NY/NJ.

Tables 3 and 4 below illustrate the program activities and guest speakers for each week of the 2017 SRI.

Table 3. SRI 2017 Program Activities Weeks One to Eight

Schedule	Topic	Faculty /Guest Speakers	SRI 2017 Activities
WEEK ONE June 5 – 9	MTS and Maritime Security Overview	Facutly: Dr. Thomas Wakeman, Stevens Guest speaker: Dana Goward, RNT Foundation.	Discussions/lectures on maritime security and vulnerabilities. Field visits: NYC ferry terminals.
WEEK TWO June 12 - 16	Team Research Projects	Guest speakers: Bert Macesker & Susan Stevens, USCG RDC -Michael DiBartolo, NYPD -Dr. Barry Bunin, Stevens	Field-visit: CBP Port of NY/NJ. Seminar: How to conduct research 101.
WEEK THREE June 19 - 23	Team Research Projects		Field-visit: Sector Long Island Sound New Haven, CT. Experiments: Ice Fracturing Status Update Presentations.
WEEK FOUR June 26 – 30	Team Research Projects		Experiments: USV stability test Status Update Presentations.
*Note that activities after July 1 for the SRI are considered planned activities for Year 4, but are reported here for consistency and program continuity.)			
WEEK FIVE July 5 – July7	Team Research Projects		Experiment: Stevens Anechoic Chamber.
WEEK SIX July 10 – 14	Team Research Projects		Experiment: ROV Deployment -Status Update Presentations
WEEK SEVEN July 17 - 21	Research Synthesis		Report writing, presentation slide preparation and research posters. -Status Update Presentations
WEEK EIGHT July 24 – 28	Team Reports	MSC representatives and Invited stakeholders & DHS guests	Final reports & presentations

Table 4. SRI 2017 Guest Speakers

Guest Speaker	Organization	Lecture Topic
Dana Goward	Resilient Navigation and Timing (RNT) Foundation	GPS Vulnerabilities
Bert Macesker, Executive Director & Susan Stevens, Resource Director	U.S. Coast Guard Research and Development Center	USCG Missions and R&D Project Portfolio
Michael DiBartolo, Officer	NYPD-Counterterrorism Division	Port Awareness and Security Threats

3.4.6. SRI Field Visits and Meetings with Practitioners

Field visits to ports and homeland security facilities are a key component of the Summer Research Institute. Field-visits provide a first-hand opportunity for students to observe the operational activities and responsibilities of homeland security professionals in the field (see Figure 4 below).

Figure 4. SRI 2017 students prepare for a trip aboard a Coast Guard vessel at Sector Long Island Sound.

During the 2017 SRI, students participated in field-visits and engaged in activities with representatives from the following homeland security organizations:

- Customs and Border Protection (CBP) Field Operations Division (Field-visit)
- U.S. Coast Guard Sector Long Island Sound (SLIS) (Field-Visit)
- Port Authority of NY and NJ (PANYNJ) – NY Waterways and Staten Island Ferry (Security Observation Exercise)

This was the SRI's sixth annual field-visit to CBP at the Port of NY/Newark and the first annual visit to USCG SLIS. The visit to CBP included observations of radiation portal monitors in use, high-energy mobile non-intrusive inspection (NII) equipment scanning cargo containers, and a tour of a Centralized Examination Station warehouse where cargo is physically inspected and analyzed. New to this year's visit, was a demonstration of CBP's canine unit and the ability to observe CBP Officers deploy a remotely operated vehicle (ROV) during a simulated pier inspection.

The trip to SLIS included a discussion with the Sector Commander, CAPT. Andrew Tucci, as well as a tour of the Command Center, a review of the Aids to Navigation (ATONS) unit, and a trip aboard a Coast Guard vessel.

Field-visits and networking opportunities like the CBP and SLIS visits, have resulted in invitations for students to attend other local and regional homeland security practitioner activities. Prior to the start of the SRI, the students were invited to attend NUSTL's second-annual Urban Operational Experimentation and at the culmination of this year's program, the students have been invited to attend a Cybersecurity Workshop hosted by the Sector New York Area Maritime Security Committee, and a full-scale active shooter exercise at the Lincoln Tunnel, hosted by the PANYNJ.

3.4.7. SRI 2017 Student Research Projects

In planning for the SRI 2017 program, MSC researchers and administrators reached out to stakeholders at the USCG RDC and to CBP to gather information on projects of interest to them. Conversations with the USCG RDC, together with the Center's research in maritime cybersecurity (e.g. the NSF funded project and the ABS maritime cybersecurity project) inspired the framework for the SRI Maritime Cybersecurity project. Conversations with CBP Officers regarding the detection of parasitic devices on ship hulls and pier pilings, led to the development of the ROV and Virtual Reality projects. The Arctic Acoustics project was developed in part by research completed by MSC's Maritime Security Fellowship student Tyler Mackanin and with the Center's research in the area of passive acoustic systems in mind. The projects and student team assignments are described below.

Research Team/Project: Maritime Cybersecurity – Data Flows in the MTS

Figure 5. Catherine Javadian, Jennifer Li & Dylan Luzzolino (l to r) conducted research on the Maritime Cybersecurity Team.

Cybersecurity vulnerabilities and threats to the Maritime Transportation System (MTS) are of significant concern to the USCG and to the maritime and port community. In 2016, Stevens Institute of Technology together with support from the MSC, were awarded an NSF grant to develop program curriculum and student research opportunities focused on Maritime Cybersercurity. As part of the NSF project, a team of students was formed during the Center's 2017 SRI to investigate data exchanges in the MTS in order to allow the identification of inadvertent information flows.

Utilizing recent mappings of the maritime and port community, the team worked to identify the types of data exchanged during the export process. Given the proprietary nature of the data, the students utilized open source information to diagram data flows and the types of data exchanged in the process. The team was able to document several steps in the export process and to find more than 100 different types of data exchanged between port partners throughout the export process.

A copy of the team's final presentation slides can be found on the Center's website at: *https://www.stevens.edu/SummerResearchInstitute.*

Table 5. Maritime Cybersecurity – Student Team

Student	Academic Discipline	School
Dylan Luzzolino	Cybersecurity	Stevens Institute
Jennifer Li	Computer Science	University of Alabama - Huntsville
Catherine Javadian	Cybersecurity	Stevens Institute

Faculty Mentors: Drs. Susanne Wetzel and Thomas Lechler, Stevens Institute

Research Team/Project: Arctic Acoustics – Detecting and Localizing Changes in Ice Cover

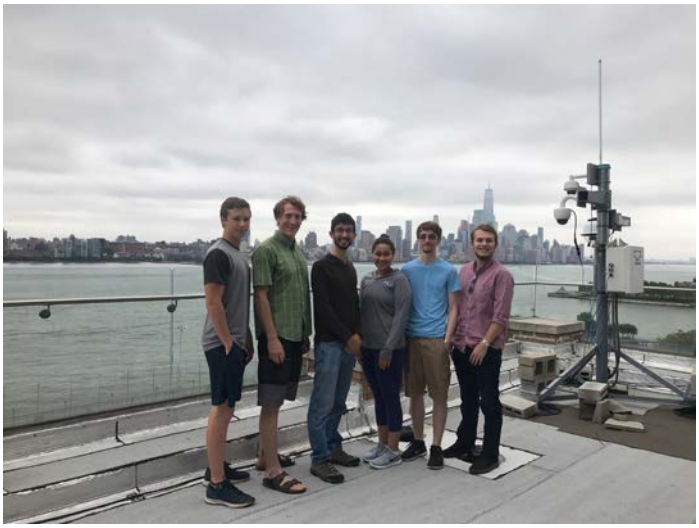


Figure 6: Students on the SRI 2017 Arctic Acoustics Team

Over the past several years, reductions in ice coverage in the Arctic region have increased the number of vessels transiting the newly-formed Northwest Passage. The increasing numbers of commercial (e.g., oil tankers and cargo ships) and leisure vessels (e.g. cruise ships) in the region are placing greater demands on the U.S. Coast Guard to ensure safe and secure navigable waters and to conduct greater numbers of search and rescue missions. Students on the SRI 2017 Arctic Acoustics team aimed to assess if underwater passive acoustic systems could be utilized as an approach to enhance the Coast Guard's Maritime Domain Awareness in the Arctic by detecting and localizing sounds made by changes in ice composition. (e.g., ice fractures, ice shear deformations and floes). Being able to identify the acoustic signature of ice cracking in real-time would have the potential for helping the Coast Guard and other vessels navigate the Arctic by identifying moving ice-floes and the persistent monitoring of ice conditions.

As part of their research, the team studied the fundamentals of acoustics including acoustic wave parameters, propagation principles and acoustic wave reception and analysis, and conducted more than 125 experiments over the course of eight weeks to simulate and record sounds made by ice under variable simulated environmental conditions.

The team's research outcomes demonstrated the potential for underwater passive acoustic systems to be used to detect and identify sounds made by changing behaviors in ice. In particular, thermal cracking, fracturing and shearing. Details regarding the

team's research methodology and project outcomes can be found in their final research report and presentation slides on the MSC website at: *https://www.stevens.edu/SummerResearchInstitute*

Table 6. Arctic Acoustics Student Research Team

Student	Academic Discipline	School
Matthew Alrichs	Civil Engineering	University of Alaska - Anchorage
Trevor Hinds	Mechanical Engineering	Stevens Institute
James Lyons	Chemical Engineering	Stevens Institute
James Matthews	Civil Engineering	University of Alaska - Anchorage
Stephen Opet	Electrical Engineering	Stevens Institute
Khiana Rogers	Civil Engineering	Northeastern University
Faculty Mentors: Dr. Barry Bunin, Dr. Marehelli Prasad, and Mr. Chenhui Zhao, Doctoral Candidate		

Research Team/Project: Virtual Reality and Its Applications to Maritime and Port Security

Figure 7. Students on the VR team take a break for a photo-op in the Lab.

Students on the Virtual Reality (VR) team conducted research on the applications of VR to maritime and port security operations. Currently being used to train emergency responders to array of crisis events, the team aimed to create underwater environments

utilizing VR Headsets to assist homeland security practitioners to prepare for and respond to underwater safety and security operations. (e.g. the inspection and search for parasitic devices). VR environments allow homeland security professionals to efficiently and effectively gain valuable training experience without being placed into harm's way, or jeopardizing the damage to expensive response tools and technologies.

The goal of the team's project was to create VR environments that simulated the use of Remotely Operated Vehicles (ROVs) as they perform inspections of vessels and pier pilings for security threats or parasitic devices. Leveraging equipment provided by the MSI summer research team from the University of Texas Rio Grande Valley, and from Stevens Sensory Computation, Experimental Narrative Environments (SCENE) Lab, the team created several interactive 3D environments, as well as scenarios that integrated visualized real-time data into VR. The team's research methodology and project results can be found in their final research report and presentation slides on the MSC website at *https://www.stevens.edu/SummerResearchInstitute.*

Table 7. Virtual Reality – Student Research Team

Student	Academic Discipline	School
Michael Alecci	Mechanical Engineering	Stevens Institute
Victor Carreon	Mechanical Engineering	Univ. of TX – Rio Grande Valley
Nicholas Duca	Finance	Stevens Institute
Juan Elizondo	Industrial Engineering	Univ. of TX – Rio Grande Valley
Jared Hobbie	Cybersecurity	Stevens Institute
Vincent Lee	Computer Science	Stevens Institute
Daniel Odell	Computer Science	Elizabeth City State Univ.
Gabrielle Padriga	Computer Science	Stevens Institute
Faculty Mentors: Dr. Alley Butler, UTRGV and Blaise Linn, Stevens Institute		

Research Team/Project: Remotely Operated Vehicle (ROV) and Unmanned Surface Vehicle (USV) Cooperation in Maritime and Port Environments

Figure 8: The ROV/USV research team conducts research in the Robotics and Automation Lab at Stevens.

Students on the ROV/USV team conducted research into the use of Remotely Operated Vehicles (ROV) and Unmanned Surface Vehicles (USVs) to conduct the inspection of maritime structures for parasitic devices and structural integrity. The team was particularly tasked with integrating these technologies to develop a platform whereby the USV could serve as an autonomous mothership for the ROV during inspections.

To accomplish their tasks, the students organized themselves into three subgroups. The USV group was responsible for assessing the capabilities and limitations of the system to carry sensor platforms, the ROV Mechanical Analysis group was responsible for creating (machining) the equipment mounts needed to attach the Doppler Velocity Log (DVL) sensor to the ROV and lastly, the ROV Software group was responsible for integrating the DVL sensor with the VideoRay ROV's Position Management System.

Throughout the summer, the team conducted several joint experiments that included the testing of the USV in the Stevens Aquatic Center to determine the optimal placement of sensor equipment under variable wave conditions. Other experiments included the deployment of the ROV the Hudson River adjacent to Stevens to test the ROV/DVL mounting system in the harsh Hudson River currents, and the collection of data through the software system. The team's research methodology and project results can be found in their final research report and presentation slides on the MSC website at *https://www.stevens.edu/SummerResearchInstitute*.

Table 7. ROV/USV Student Research Team

Student	Academic Discipline	School
Kyle Alvarado	Mechanical Engineering	Univ. of Alaska – Anchorage

James Fredericks	Marine Operations	SUNY Maritime
Mathew Green	Naval Engineering	Stevens Institute
Victoria Kapp	Mechanical Engineering	Stevens Institute
Anthony Orrico	Computer Engineering	Stevens Institute
Max Panoff	Electrical Engineering	Stevens Institute
Faculty Mentor: Dr. Brendan Englot, Stevens Institute of Technology		

3.4.8. SRI 2017 Student Survey

An assessment of the 8th annual summer research program was conducted via a student survey (see Appendix E-2 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 strengths and weaknesses of the program, the student's learning gains over the eight-week program, areas for program improvement and program impacts on student interest in advanced study and/or careers in homeland security. 20 students out of the 22 participants completed the program survey.

A majority of the student respondents rated the SRI "Excellent" in the following categories:

- Quality of Field Trips (100%)
- Quality of Program Coordination/Administration (85%)
- Quality of Guest Lectures (75%)
- Ability to be Innovative and Self Motivated (70%)
- Quality of Teamwork (70%)
- Quality of Research Facilities (70%)
- Faculty Mentor Guidance and Assistance (65%)
- Quality of Program Curriculum (65%)
- Quality of Faculty Lectures (65%)
- Quality of Research Outcomes (60%)

95% of the survey respondents (20 out of the 22 students) said 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:

- Ability to Conduct Research (65%)
- Teamwork/Collaboration (60%)

When asked to reflect on their "Top 3 Takeaways" from the program, the students commonly mentioned the following:

- Increased ability to conduct research,
- Enhanced Oral Presentation Skills,
- A better understanding of the complexities of the maritime domain.
- Student relationships

Suggested areas for improvement included the request for more networking opportunities and orientation lectures tailored more specifically to the summer's research projects, rather than a broad overview of the maritime domain.

The students worked in close collaboration with MSC researchers and had the unique opportunity to interact and engage with maritime industry and homeland security practitioners. Through their experience in the summer research program, students gained a greater awareness of maritime security issues and the vital role of the MTS to the nation's economy. Student survey responses show that participation in the SRI has effectively inspired student interest to pursue careers and study in the homeland security domain. Collectively, the SRI was effective in achieving the following outcomes:

- Student presentations and research reports demonstrated the students advanced knowledge and understanding of the maritime security domain.
- Students enhanced their professional skills by providing weekly research presentations.
- A majority of the students (95%) expressed enhanced interest in pursuing careers and/or advanced academic study in maritime/homeland security as a result of their participation in the SRI.

3.4.9. SRI Lessons Learned

MSC continuously strives to enhance the learning experiences of its student participants by modifying and adjusting the SRI program format. For this year's program, the Center increased the amount of student research time by reducing the number of in class lecture assignments. The program administrators also leveraged broader faculty engagement across the Stevens Institute of Technology research enterprise. This year, faculty members from the Schools' of Engineering, Business and Arts and Letters provided additional mentorship and resources for the student research projects. Broader faculty participation resulted in greater access to research assets and helped to inspire potential research collaborations among Stevens faculty and the MSC.

3.5. Maritime Security Master's and Doctoral Fellowship Programs

Milestones	Performance Metrics	Status/Discussion
1. Homeland Security Graduate Research Assistantship 6/1/16 – 12/30/16	Conduct recruitment and outreach. Confer a minimum of one Graduate Research Assistantship.	Partially completed: MSC awarded an Undergradu-

		ate Research Assistantship in lieu of a graduate assistantship.
2. DHS CDG Fellow placement in a field-based internship. 6/1/16 – 8/30/17	Place (one eligible) student in a ten-week field-based internships with a DHS component agency.	Completed: Tyler Mackanin engaged in a ten-week internship with HSSAI.
3. Master's & Doctoral Degree Fellows fulfill fellowship requirements. 7/1/16 – 6/30/17	Master's & Doctoral Degree Fellows maintain GPA and fulltime enrollment. Graduating Fellows (one eligible student) complete coursework and thesis requirements, and assume position in the HS enterprise. Student employment and professional activities will be tracked through a post-program survey.	Completed: All students maintained GPA and fulltime enrollment requirements. Completed: Tyler Mackanin successfully completed his thesis and degree requirements to receive his Master's in Maritime Systems Completed: Tyler Mackanin has assumed a fulltime Research Assistant position at Stevens Institute of Technology, while pursuing career opportunities in the HS enterprise.
4. Career placement and post-program tracking. 6/1/16-6/30/17	CDG fellowship alumni employment and professional activities will be tracked through a post-program survey.	Completed: A fellowship alumni survey was sent to 8 of the nine eligible fellows. All eight responded to the survey.
5. Doctoral Fellows Research Symposium.	Hold Doctoral Fellows Research Symposium in conjunction with MSC stakeholder meeting.	Partially Completed: In lieu of holding the doctoral research symposium as part of an MSC stakeholders meeting, MSC doctoral fellows presented their research at the Stevens Graduate Research Conference.

3.5.1. MSC Supported Students

In addition to the five students supported by the MSC during the 2017 Summer Research Institute, the Center also provided support for two students in the form of Re-

search Assistantships. Blaise Linn conducted research with the MSC as a Graduate Research Assistant and Dmitriy Savinskiy, served as an Undergraduate Research Assistant.

During the 2016/2017 academic semester, Blaise Linn engaged in 20 hours per week of research with the Maritime Security Center, and successfully completed his degree requirements to receive a Master's of Science in Maritime Systems from Stevens Institute of Technology in May 2017. Throughout his Graduate Assistantship, Blaise provided research support on projects related to mobile, modular sensor platforms that can be used to bolster Maritime Domain Awareness (MDA) for the U.S. Coast Guard and other DHS component agencies. He also completed a master's thesis titled *Requirements and Hardware Elements for an Acoustic Smart Buoy.* While pursuing full-time employment in the homeland security domain, Blaise has assumed a short-term position with Stevens Institute of Technology to continue his research of the Center's projects and to provide mentorship to a team of students in the Center's 2017 Summer Research Institute.

Dmitriy Savinskiy was selected as an Undergraduate Research Assistant, based on his superior academic performance in the Stevens Institute of Technology Electrical Engineering program. He currently possesses a cumulative GPA of 3.9 out of 4 and is an alumni of the Center's 2014 Summer Research Institute. Throughout the 2016/2017 academic year, Dmitriy provided 20 hours of research support per week, working on projects related to mobile, modular sensor platforms and AIS spoofing and fraud detection. As a result of Dmitriy's outstanding work and research capabilities, the Center has extended his Undergraduate Research Assistantship into the 2017/2018 academic year. He is currently a rising senior and anticipates to complete his degree requirements in May 2018.

3.5.2. Mechanical Engineering and Homeland Security Doctoral Fellowship – DHS Career Development 2015 Supplement Award

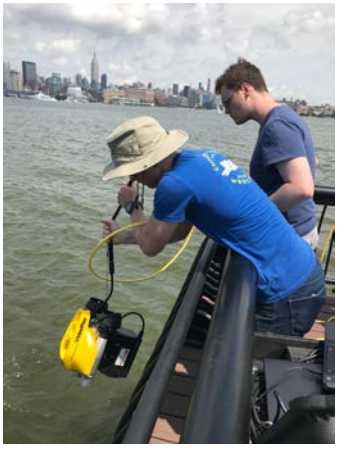


Figure 9. Doctoral Fellow, John Martin tests the odometry readings from sensors on an ROV.

Mr. John Martin was selected to receive the Center's Mechanical Engineering and Homeland Security Doctoral Fellowship in the fall of 2015. He is currently entering his third year in the Mechanical Engineering Doctoral program, where he is conducting research in conjunction with his dissertation advisor, Dr. Brendan Englot, Assistant Professor, Mechanical Engineering. During the 2016/2017 academic year, John completed 24 additional credits towards his PhD requirements and engaged in the following courses and fellowship activities:

Semester	Courses/Activities	Credits
Spring 2017	CS559: Machine Learning: Fundamentals and Applications	3
Spring 2017	CS505: Probability and Stochastic Processes	3
Spring 2017	ME960: Mechanical Engineering Doctoral Research	6
Fall 2016	ME960: Mechanical Engineering Doctoral Research	3
Fall 2016	CS541: Artificial Intelligence	3
Fall 2016	MA502: Mathematical Foundations of Computer Science	3

Fellowship and Research Activities:

- Provided a guest lecture on Reinforcement Learning Algorithms to the Stevens ME654: Advanced Robotics class.
- Designed a reinforcement learning algorithm to support autonomous patrolling operations of an underwater robot.
- Presented research results of camera vision experiment to representatives from the USCG Sector New York Safety and Security Division at a MSC stakeholder meeting in December 2016.
- Conducted experiments in Stevens Davidson Laboratory to collect and analyze ROV camera vision data.

Publications and Posters:

- Submitted a conference paper titled *Extending Model-based Policy Gradients for Robots in Heteroscedastic Environments* for consideration to the 2017 Conference on Robotic Learning
- Submitted a conference paper titled *A Deterministic Policy Gradient Algorithm for Robots in Heteroscedastic Environments* to the 2017 International Conference on Intelligent Robots and Systems

- Presented a poster titled *Predicting Ocean Currents for Robot Navigation* at the Stevens Institute of Technology Graduate Research Conference – Spring 2017
- Submitted a research paper titled *A Policy Gradient Method for Reducing Localization Uncertainty in Cyclic Patrolling Tasks* to the 2016 International Conference on Robotics and Automation

Over the coming academic year, John will continue to enroll in classes full-time and will complete additional research contributing to his dissertation.

3.5.3. Maritime Security Doctoral Fellowship - DHS Career Development 2013 Supplement Award

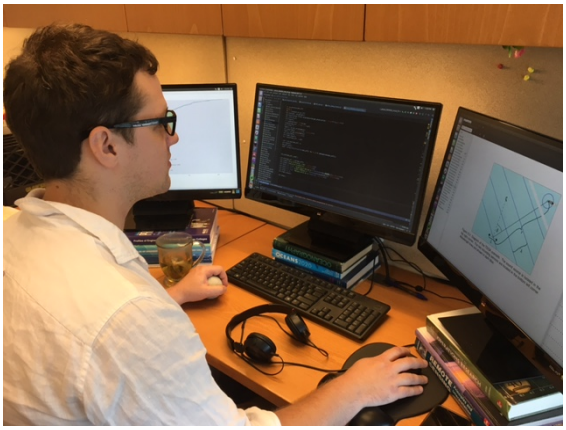


Figure 10. Alex Pollara prepares to defend his dissertation in the area of characterization and identification of small vessels from underwater sound.

Alex Pollara was awarded the Maritime Security Doctoral Fellowship in June 2014. Over the past three years, Alex has been conducting research leading to a doctoral dissertation in the area of characterization and identification of small vessels from underwater sound. During the 2016/2017 academic year, Alex completed 18 additional research credits towards his degree, to fulfill his credit requirements for the Stevens Ocean Engineering doctoral degree program. He is currently scheduled to defend his doctoral dissertation in August 2017.

Throughout the 2016/2017 academic year, Alex engaged in the following fellowship and research activities:

Fellowship and Research Activities:

- Defended dissertation proposal and commenced the writing of his dissertation.
- Presented a conference paper on *Passive Acoustic Methods of Small Boat Detection, Tracking and Classification* at the 2017 IEEE International Symposium on Technologies for Homeland Security in Waltham, MA. This paper was published in the conference proceedings.

- Selected to present research titled *Specifics of DEMON Acoustic Signatures for Small and Large Boats* at the 2017 Acoustical Society of America Conference in Waltham, MA.
- Selected to present a research paper titled *Improvement of the Detection of Envelope Modulation on Noise and its Application to Small Boats* at the Oceans 2016 conference sponsored by the Marine Technology Society and IEEE Oceanic Engineering Society in Monterey, CA.
- Selected to present research on two topics titled *Feature Extraction of Acoustic Signatures of Small Boats*, and *Phase DEMON Algorithm for time delay Estimation used in Small Boat Tracking* at the Acoustical Society of America Conference held in Honolulu, HI

Publications and abstracts:

- Published a peer reviewed journal article titled *Modulation of High Frequency Noise by Engine Tones of Small Boasts*, in the July 2017 issue of Journal of Acoustical Society of America.
- Published a peer reviewed journal article titled *Clippers, yachts, and the false promise of the wave line,* published in the July 2017 edition of Physics Today

Complete citations for Alex's journal articles can be found on the MSC website at https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/reports-publications

Alex will defend his doctoral dissertation, *Characterization of Small Vessels from Acoustical Signatures*, this August 2017. At the time of his dissertation defense, Alex will have successfully fulfilled his degree and fellowship requirements. He is currently pursuing employment opportunities within the homeland security enterprise.

3.5.4. DHS Career Development Grant Master's Degree Fellowship – 2012 Award

In Year 3, Tyler Mackanin served as the last remaining student in the MSC Maritime Systems Master's Degree Fellowship program. Throughout the 2016/2017 academic year, Tyler completed the remaining credits for his degree program and defended his master's thesis titled *Arctic Ice Sound Detection and Localization – How can ice-generated sounds be identified and localized to enhance Maritime Domain Awareness?*

In May 2017, Tyler Mackanin successfully fulfilled his fellowship and degree requirements to receive a Master's of Science in Maritime Systems with a Graduate Certificate in Maritime Security. During the 2016/2017 academic year, Tyler engaged in the following courses and fellowship/research activities.

Semester	Course	Credit
Spring 2017	OE900: Maritime Security Thesis	3

Spring 2017	SYS581: Introduction to Systems Engineering	3
Fall 2016	OE900: Maritime Security Thesis	3
Fall 2016	OE511: Urban Oceanography	3
Summer 2016	Field-based Internship: Homeland Security Studies and Analysis Institute (June – August 2016)	

Fellowship and research activities:

- Completed and defended master's thesis.
- Provided research support on MSC research projects related to mobile, modular sensor platforms.
- Attended the Association for Unmanned Vehicle Systems International (AUVSI) Conference in Dallas, TX.
- Provided volunteer support to the Port Authority of NY/NJ Active Shooter full-scale exercise held at the Bayonne Cruise Terminal.

Upon graduation from the Maritime Security program, Tyler assumed a fulltime Research Assistant position with Stevens Institute of Technology, where he is providing support to Stevens research faculty in the area of unmanned systems. Tyler's ultimate goal is to pursue long-term employment with the U.S. Coast Guard.

3.5.5. Maritime Systems Master's Degree Fellowship – Alumni Survey

In the spring of 2017, MSC prepared and distributed a post-program survey to seven of the Center's nine Master's Degree Fellowship alumni. The survey was designed to track the homeland security employment and career activities of the Center's fellowship students following the completion of their degree programs. Surveys were not distributed to two of the program students, as one was in the process of completing the program and therefore had not yet joined the workforce and the other had graduated from the fellowship program and entered directly into a doctoral program.

Survey responses confirmed that all seven of the students had successfully completed or were in the process of completing their one year post-program employment requirement in the homeland security domain. Students reported that on average, it took them two to four months to obtain their first homeland security position and the primary source for finding their jobs was through contacts facilitated through MSC's personnel/leadership and USA Jobs. A majority of the students reported that their primary job responsibilities were technical in nature (83%) and when asked how they would compare their skills and knowledge to their coworkers/peers, 57% replied that "*the Fellowship program provided me with more technical knowledge, skills and experience than my counterparts".* Six of the seven survey respondents reported that they were still employed in positions directly with or in support of the Federal government. Of the six students, three reported employment with DHS component agencies (e.g. USCG RDC and

NUSTL), one reported employment with the DOE (e.g. Pacific Northwest National Laboratories), one with the DOD (U.S. Army Redstone Arsenal), and one at Stevens Institute of Technology, working in a maritime/homeland security research capacity. A copy of the Fellowship Alumni survey can be found in Appendix E-2.

3.5.6. MSI Outreach and Engagement in Research

Milestone	Performance Metrics	Status / Discussion
1. Minority and women student participation in the Center's annual Summer Research Institute. SRI 2017 – outreach and recruitment (9/1/16 – 2/26/17)	Diversity in the SRI program will reflect a minimum of 50% of students from underrepresented communities. (e.g. minority students, women and MSI enrolled students.)	Incomplete: The demographics for the 2017 SRI included 36% students from underrepresented communities and students from two MSIs.
2. MSI participation in MSC research activities/programs. Summer Research Team program YR 3 (6/5/17 – 8/11/17)	MSC will host a minimum of one MSI SRT team per summer. - Outreach efforts to recruit MSI SRT participation will be measured by the number of targeted email distributions and personal conversations had with MSI representatives.	Completed: MSC hosted faculty and students from UTRGV in the 2017 MSI SRTP.

Figure 11. Dr. Butler, Professor (l) together with master's degree students Juan Elizondo (c) and Victor Carreon (r) conducted research with the MSC through the DHS MSI SRTP.

MSC in conjunction with a faculty and student research team from the University of Texas Rio Grande Valley were selected to participate in the DHS OUP Minority Serving

Institutions (MSI) Summer Research Team Program. The ten-week summer research program was held on-campus at Stevens Institute of Technology and included research into the uses of virtual reality applications to support homeland security training and field-based operations. The MSI SRTP program was held concurrent to and in conjunction with the Center's 8th annual Summer Research Institute. The conjoining of the two programs afforded the MSI summer research team with the added benefit of being able to engage in the program's coordinated field-visits to DHS component agencies (CBP Field Operations and USCG Sector Long Island Sound) and to participate in the SRI faculty and guest lectures among other activities.

The MSI UTRV team completed an exhaustive literature review into the science behind and multi-use capabilities of VR. The team also collaborated with students from the Center's 2017 SRI Virtual Reality team to begin to develop VR environments focused on the inspection of ship hulls for parasitic devices. At the time of this report, the MSI SRTP team is in the process of completing their required research report and preparing for a final research presentation for MSC research members and DHS stakeholders. The UTRGV team in collaboration with faculty members from Stevens Mechanical Engineering Department, plan to pursue DHS OUP follow-on funding to continue their research in this area.

During Year 3, the Center also prepared letters of support for two MSI schools applying for the DHS OUP Scientific Leadership Awards. The schools included Elizabeth City State University and Texas Southern University. Decisions regarding the Scientific Leadership Awards were not completed during the 2016/2017 academic year due to DHS OUP budget reasons.

4. 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, Biennial Review, management, and guidelines and policies.

4.1. Project Solicitation

During this year, MSC used all its available resources to solicit projects. This included meetings with members of the DHS S&T Borders and Maritime Division (BMD), development of an RFP to be issued in Year 4, meetings with a number of DHS operational components and stakeholders, and development of a number of White Papers to address problems of interest to DHS and its components.

MSC PI met and corresponded with members from the BMD at multiple occasions to discuss Coast Guard and Customs and Border Protection gaps that are related to maritime security. The gaps discussed included the research questions that were posed in the original COE Funding Opportunity Announcement as well as Integrated Product Team (IPT) and sub-IPT gaps identified as high priority items. The discussions led to a

number of White Papers that were generated by MSC and sent to the Program Manager. One of these papers led to the approval of the VTS Radar Research Project.

In anticipation for Year 4 projects and at the recommendation of the Program Manager, MSC prepared an RFP along with the process that includes the announcement, guidelines, and the review process. The RFP will be issued early in Year 4 to solicit COE projects that address IPT gaps and FOA research questions.

MSC PI and other MSC researchers met with DHS stakeholders and developed a number of White Papers to address their concerns. The stakeholders that were involved included USCG Sector NY, USCG Sector LI, USCG CG-MLE, USCG RDC, USCG Sector Corpus Christi, CBP Air and Marine, CBP Newark, Plum Island Animal Disease Center, JFT-N, and JIATF-S. In addition, these topics were presented at the MSC Biennial review. The topics proposed as projects include:

1. Dark Vessel Detection
2. Protection of MPAs (Marine Protected Areas)
3. Acoustic Sensors for Arctic Applications
4. Detection of Illegal Port Activities
5. Multi-sensor for Illegal Shore Activities
6. Off-shore Wind Turbines Interference
7. Enhanced Communications Through Hazards
8. RF Surveillance of Ships
9. AIS Behavioral Analysis
10. Game Theory for Enhancing Drug Interdiction
11. Underwater Hull Inspection
12. Underwater Infrastructure Inspection
13. Detection of Hazardous Materials
14. Protecting HVAs against UAS Threats

Despite the operational components high level of interest in these topics, the projects were not moved forward due to the inability to find a project champion at the CG HQ level and lack of interest from the Biennial Board of Directors.
.

4.2. Stakeholder Engagement, Communications, and Outreach

MSC continued to host visitors and partners with various key stakeholder organizations in a range of activities (e.g., Meetings, trainings and exercises). MSC has partnered with

the USCG RDC, USCG Sector NY, Borders and Maritime, Customs and Border Protection, National Urban Security Technology Lab, the NYC Police Department, NJ Office of Homeland Security and Preparedness, and others as described below.

USCG RDC

USCG RDC representatives served as guest speakers during the 2017 Summer Research Institute. In addition, RDC served as a trusted partner for discussing various Center projects (both existing and proposed) and their relevance to the Coast Guard.

USCG Sector New York

MSC's Director of Education has been serving as a co-Chair for the Sector NY Area Maritime Security Committee – Cybersecurity Subcommittee. The Sector New York AMSC Cybersecurity Subcommittee was formed to support the Coast Guard's Cyber Strategy and to enhance the cybersecurity awareness and posture of the Port of New York/New Jersey. The Committee organized and delivered three Cybersecurity-focused tabletop exercises for the Port of NY/NJ in August 2017, one of which was hosted by the MSC at Stevens Institute of Technology. Throughout Year 3, the Committee continued to meet and plan for a NY/NJ port-wide Cybersecurity Workshop and Cyber Gaming event. MSC's Director of Education, together with the Center's colleagues from LSU received a letter of citation from Captain Michael Day for their contributions to the Sector NY maritime and port community.

In addition to the AMSC partnership, MSC and Sector NY representatives interacted on a few occasions to discuss the Sector's operational concerns, including underwater inspections, compliance of ships, and other maritime safety and security areas of interest.

Borders and Maritime

MSC PI and other researchers met with the Director of the S&T Borders and Maritime Division to solicit input from their interactions with the DHS components (USCG, CBP, and ICE) on their operational needs. These discussions include the IPT gaps, existing projects, as well as potential new projects that can quickly fill in gaps that need to be addressed.

NUSTL

MSC administrators and students participated in NUSTL's second annual Operational Experimentation (OpEx) Exercise. Two graduates from the Center's CDG-funded Maritime Security Fellowship program were employed by NUSTL and assisted in the coordination and the test and evaluation of technologies during the OpEx event.

In addition, NUSTL served as a Center partner engaging in numerous activities and conversations with the MSC regarding areas of mutual interest.

CBP

MSC representatives were invited to meet with the CBP Port Director and Chief of Staff to discuss opportunities for collaboration and joint field experiments.

CBP's Office of Field Operations at the Port of NY/NJ hosted MSC students and faculty mentors from the 2017 Summer Research Institute for a tour of the agency's cargo scanning equipment and facilities, and for a demonstration of the agency's Remotely Operated Vehicles used for inspecting piers and ships hulls.

CBP Officers discussed research ideas and projects with MSC administrators and students.

NYPD-Counter Terrorism Division

MSC administrators and students were invited to join Hoboken Fire Department, together with other local emergency response groups, for a Port Awareness and Response training course hosted by the NYPD-CTD.

In addition, MSC PI met with NYPD officers to discuss threats that are of interest to DHS as well as ways to potentially mitigate them.

NJ OHSP

MSC in conjunction with representatives from the NJ Office of Homeland Security and Preparedness (NJ OHSP) assisted in the facilitation of several Cybersecurity tabletop exercises tailored to the Port of NY/NJ.

Other Activities

MSC also hosted a delegation of Maritime Security and Maritime Industry representatives from the Canadian Government (from the Newfoundland and Labrador Province) for a briefing and discussion on areas for future collaboration. The Canadian delegation's visit was a result of contacts made at a DHS OUP Technology Showcase in which the Center demonstrated its Passive Acoustic Detection System. The MSC PI was also invited to be one of the keynote speakers at their international conference to promote stakeholder collaboration, technological innovation, harsh environment research and development, and education efforts.

In addition to the above, MSC conducted many targeted communications activities. This included participation in the following events:

- 8th Annual Maritime Risk Symposium – Chapel Hill, NC

- PANYNJ full-scale Active Shooter Exercise – Bayonne Cruise Terminal
- FAU Port Resiliency Workshop – Dania Beach, FL
- Maritime and Arctic Safety and Security Conference – Keynote Presentation – Canada
- DHS OUP Transition Meeting – Minneapolis, MN
- COE Leadership Meeting – Hosted by the Borders, Trade, and Immigration Institute at the University of Houston, TX
- MSC Annual Meeting, where DHS OUP representatives and stakeholders from CBP, Coast Guard, and DHS S&T's Borders and Maritime Division attended – Washington, DC

The Center also generated and distributed a bi-monthly newsletter. The newsletter contains relevant information regarding the Center's research, stakeholder engagements and student achievements.

4.3. Biennial Review

MSC completed a multi-phase biennial review organized by DHS S&T's Office of University Programs. MSC was one of the first COEs to undergo such a review. The process included a series of preliminary activities leading to a three-phase review including a Letter Review, a Federal Coordinating Committee (FCC) Review, and an OUP Management Review. The FCC Review took place on March 15, 2017, at the USCG Headquarters in Washington, DC. The Center's research projects and educational portfolio were assessed and determinations regarding which projects are to move forward were made. Updates to the Center's research project and educational program portfolio were implemented prior to the Center's 4th Year. The letter review called for the elimination of a few projects and facilitated an opportunity for the Center to present new projects to the reviewers. These included the following:

a) Dark Vessel Detection

b) Protection of MPAs (Marine Protected Areas)

c) Acoustic Sensors for Arctic Applications

d) Detection of Illegal Port Activities

e) Multi-sensor for Illegal Shore Activities

f) Off-shore Wind Turbines Interference

g) Enhanced Communications Through Hazards

h) RF Surveillance of Ships

i) AIS Behavioral Analysis

j) Game Theory for Enhancing Drug Interdiction

k) Underwater Hull Inspection

l) Underwater Infrastructure Inspection

m) Detection of Hazardous Materials

n) Protecting HVAs against UAS Threats

4.4. 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 develop 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 him on a weekly 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 frequent meetings with individual PIs as well as coordinated conference call meetings with the Center's PIs every six weeks. 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.

Members the Center Science and Education Advisory Committee (SEAC) have been engaged throughout the year and were kept informed of the Center activities. They participated in conference calls with the Center management and provided input and advice to the Biennial Review. In addition, they were invited to Center activities including the annual meeting and the Summer Research Institute.

For faculty exchanges, the Center hosted an MSI Summer Research Team from the University of Texas Rio Grande Valley. The team participated in the Center's Summer Research Program for ten weeks at Stevens Institute. The Center also had some discussions with faculty from the USCG Academy, but these discussions did not lead to any exchanges during the reporting period.

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. Also, the Director discussed transition ideas with CG RDC and CBP Air and Marine personnel to understand their needs and their limitations in preparation for transitioning projects when they are ready.

4.5. 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 3 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.

Appendix R-1 – Port Resiliency Bibliography

Beatley, T. (2009). *Planning for coastal resilience: Best practices for calamitous times.* Washington, D.C.: Island Press.

Cambridge Systematics, 2008. "Waterborne Freight Transportation Bottom Line" Report prepared for American Association of State Highway and Transportation http://downloads.transportation.org/AASHTO_Waterborne_Freight_COMPLETE.pdf

CMTS, 2008. National strategy for MTS, Committee on MTS.

Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). *Designing resilience: Preparing for extreme events*. Pittsburgh, PA: University of Pittsburgh Press.

Committee on U.S. Army Corps of Engineers Water Resources Science, Engineering, and Planning: Coastal Risk Reduction, Water Science and Technology Board, Ocean Studies Board, Division on Earth and Life Studies and the National Research Council of the National Academies. (2014). *Reducing coastal risk on the East and Gulf coasts.* Washington, D.C.: National Academy of Sciences.

Comprehensive Annual Financial Report (CAFR). (2015). *Port of Long Beach: Comprehensive annual financial report*. Retrieved from http://www.polb.com/finance/annualreports.asp

Conger, Sue. Process Mapping and Management. Business Expert Press, 2011.

Dixit, V., Montz, T., and B. Wolshon, "Validation Techniques for Region-Level Microscopic Mass Evacuation Traffic Simulations," Transportation Research Record: Journal of Transportation Research Board, No. 2229, 2011, pp. 66-74.

Eksioglu, B., Eksioglu, S., Allen, A., & Myles, A. National Center for Intermodal Transportation, (2009). *A simulation model to analyze the impact of crisis conditions on the performance of port operations* (10-03-09)

Holguin-Veras, J., Jaller, M., Taniguchi, E., & Aros-Vera, F. (2013, January). *The lessons from catastrophic events for post-disaster humanitarian logistic efforts: The port au prince earthquake and the tohoku disasters*. 13-1771 Trb 92nd annual meeting compendium of papers.

Gil, I. C. & Wulf, C. (Eds.). (2015). *Hazardous future: Disaster, representation and the assessment of risk.* Berlin: Walter de Gruyter.

Harbor Highlights. (1961). *Port of Long Beach Harbor Highlights,* 7(1). Retrieved from http://www.polb.com/about/history/historicalpubs.asp

International Institute for Sustainable Seaports. (2014). Sustainable design and construction guidelines. Retrieved from http://www.getf.org/our-projects-partnerships/the-international-institute-of-sustainable-seaports/

Jin, M. (2013, January 03). *Framework development for scalable and user-friendly port recovery planning simulation*. Retrieved from http://trid.trb.org/view/2010/P/1229721

Kaisar E., Hess L., and Portal-Palomo A.B., "An Emergency Evacuation Planning Model for Vulnerable Population Utilizing Public Transportation Systems" Journal of Public Transportation Vol. 15, No. 2, 45-70.

Kaisar E., and Austin M., "Synthesis and Validation of High-level Behavior Models for Narrow Waterway Management Systems" Journal of Computing in Civil Engineering, ASCE, September, pp. 373-378

Kaisar E., “A Model for Heavy Truck Freight Movement at the Intermodal Facilities in the Port of Baltimore” conference proceedings at the 7th Conference on Access Management, Park City, Utah.
Kaisar E., Pathomsiri S., Haghani A., and Kourkounaki P., “Developing Measures of US Ports productivity and Performance: Using Data Envelopment Analysis and Free Disposal Hull Approaches” conference proceedings at the 47th Transportation Research Forum, New York.
Kaisar E., Austin M., Lagakos V., Papadimitriou S., and Haghani A., “Hierarchical Object-Oriented Models for Management of Narrow Passageways” European Research Studies Journal, Volume VI, Issue (3-4), 2003, pp 95-108.
Kostro, S. S. & Riba, G. (2014). *Achieving disaster resilience in U.S. communities: Executive branch, congressional, and private-sector efforts.* Lanham, MD: Rowman & Littlefield.
Miller, J., & Wakeman, T. (2013, January). *Lessons from hurricane sandy for port resilience*. Retrieved from http://trid.trb.org/view/2010/P/1229721
Morris, L. L., & Sempier, T. (2016). Ports resilience index: A port management self-assessment. *Ports Resilience Expert Committee,* GOMSG-H-16-001. Available at www.masgc.org/ri
MTSNAC, 2006. “The Marine Transportation System and the Global Supply Chain,” Marine Transportation System Advisory Council Report.
Naghawi, H. and B. Wolshon, “Performance of Multi-Modal Evacuation Traffic Networks: A Simulation Based Assessment,” ASCE Natural Hazards Review, August 2012, Vol. 13, No. 3, pp. 196 - 204.
NOAA Coastal Service Center. 2011. Port Resilience Planning Tool. http://www.csc.noaa.gov/port/
Paul, A., & Maloni, M. (2010). Modeling the effects of port disaster. *Maritime economics & Logistics*, *12*(2), 127-146.
Petersen, D. J. (1980). *Port of Long Beach Harbor Highlights,* 4(2). Retrieved from http://www.polb.com/about/history/historicalpubs.asp
Port Everglades. (2015). *Annual commerce report.* Retrieved from https://res-1.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/2015_Commerce_Report_ADA_FINAL_3c5a5627-ba3e-4446-a43d-38f7bcef85b2.pdf
Port Everglades. (2015/2016). 2015/2016: *Facilities guide and directory.* Retrieved from http://www.bluetoad.com/publication/?i=265901
Port Everglades. (2014). *Harbor deepening and widening*. Retrieved from https://res-2.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/Harbor_Deepening_Widening_updated_May_19_2015_cb6b34e0-b406-47ca-be9b-7706134a8bf9.pdf
Port Everglades. (2014). *History*. Retrieved from http://www.porteverglades.net/about-us/history/
Port Everglades. (2014). *Master Vision Plan*. Retrieved from http://www.porteverglades.net/expansion/master-vision-plan/
Port Everglades. (2015). *Waterborne Commerce Chart*. Retrieved from https://res-4.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/2015_Waterborne_Commerce_Chart_228bb813-20cb-4b6a-a730-d337798cf7b7.pdf
Port of Long Beach. 2016. *About the Port*. Retrieved from

http://www.polb.com/about/default.asp
Port of Long Beach Annual Report. (2000). *2000 Annual Report*. Retrieved from http://www.polb.com/about/history/historicalpubs.asp
Port of Long Beach. (2016). *Facts at a Glance.* Retrieved from http://www.polb.com/about/facts.asp
Port of Long Beach. (2016). *Frequently Asked Questions*. Retrieved from http://www.polb.com/about/faqs.asp
Port of Long Beach. (2016). *Tonnage Summary.* Retrieved from http://www.polb.com/economics/stats/tonnage.asp
Port Nola. (2016). Port of New Orleans: History. Retrieved from http://portno.com/history
Port Nola. (2016). *Port Directory: The 2016 Official Directory of the Port of New Orleans*. Retrieved from http://portno.com/port-directory
Port Nola. (2016). *Port of New Orleans: Port Statistics*. Retrieved from http://portno.com/port-statistics
Portal M.I., Kaisar E.I., Golias M., and Ivey S., "Scheduling Container Vessels Under Handling and Arrival Time Uncertainty" conference proceedings at the 92th Transportation Research Board Annual Meeting, Washington DC.
Portal Palomo I., Kaisar E., "Ports as a Growing Factor in the Supply Chain", Conference proceedings at the 9th Latin American and Caribbean Consortium of Engineering Institutions, Medellin, Colombia
Pounds, B. J., Ward, K. R. & Forsythe, D. (2013). *NOAA rapid survey response for Hurricane Sandy*. Retrieved from http://ushydro.thsoa.org/hy13/pdf/0326P_10L_58.pdf
Rice, Jr., J. B., Trepte, K., Nickerson, J., Python, G., Luettich, R., & Beck, K. (2014). *Port resilience decision framework toolkit-Decision processes.* Retrieved from http://coastalhazardscenter.org/dev/wp-content/uploads/2015/03/2014-1405a-enclosure-1.pdf
Scarlatos P., Kaisar E., and Teegavarapu R., "Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems", In Mathematical Methods and Applied Computing", ISBN 978-960-474-124-3, pp. 324-346.
Stich, Bethany and Chad Miller. "Collective Action Regimes in Inland Marine Port Clusters: The Case of the Tenn-Tomm Waterway System," MS Water Resource Conference. Proceedings, 2009.
Stich, Bethany and Chad Miller. "Using the Advocacy Coalition Framework to Understand Freight Transportation Policy Change." Public Works Management and Policy. Vol. 13, No. 1, 62-74, 2008.
Stich, Bethany and Bill Martin. (2011) Measurements for Success of Container on Barge Utilization on the Tennessee-Tombigbee Waterway Prepared for: The National Center for Intermodal Transportation (NCIT)
Smongesky, P. P. (2007). Port of Long Beach Chronological History: Introduction. In C. F. Connors (Ed.), *Chronological History By Pier: 1909-2002* (pp. 1-13). Retrieved from http://www.polb.com/about/history/historicalpubs.abs
Southworth, Frank, Jolene Hayes, Shannon McLeod, and Anne Strauss-Wieder. 2014. "Making U.S. Ports Resilient as Part of Extended Intermodal Supply Chains" TRB Report. http://onlinepubs.trb.org/onlinepubs/ncfrp/ncfrp_rpt_030.pdf

Sturgis, L. A., Smythe, T., & Tucci, A. E. (2014). Port recovery in the aftermath of Hurricane Sandy: Improving Port resiliency in the era of climate change*. Center for a New American Society: Voices from the Field.* Retrieved from http://www.cnas.org/sites/default/files/publications-pdf/CNAS_HurricaneSandy_VoicesFromTheField.pdf

U.S. Government Accountability Office. (2012). Critical infrastructure protection: An implementation strategy could advance DHS's coordination of resilience efforts across ports and other infrastructure (GAO-13-11). Retrieved from http://www.gao.gov/assets/650/649705.pdf

Wakeman, III, T. H. & Miller, J. (2013). *Final report: Lessons from Hurricane Sandy for port resilience* (UTRC-RF Project No. 49997-56-24). Retrieved from http://www.utrc2.org/research/projects/hurricanesandy-port-resilience

Wang, J., Olivier, D., Notteboom, T., & Slack, B. (Eds.). (2005). *Ports, cities, and global supply chains.* Burlington, VT: Ashgate Publishing Company.

Wolshon, B., and V.V. Dixit, "Traffic Modeling and Simulation for Regional Multimodal Evacuation Analysis," International Journal of Advanced Intelligence Paradigms, Vol. 4, No. 1, 2012. pp. 71-82.

Wolshon B. and B. McArdle, "Traffic Impacts and Dispersal Patterns on Secondary and Low Volume Roadways During Regional Evacuations," ASCE Natural Hazards Review, February 2011, Vol. 12, No. 1, pp. 19 - 27.

Wolshon, B. and V.V Dixit. "Planning and Management of Transportation Systems for Evacuation," Chapter TBD, Handbook of Emergency Response: A Human Factors and Systems Engineering Approach, ISBN: TBD, Taylor & Francis Publishing Inc., New York, anticipated publication in May 2013.

Wolshon, B. and P. Murray-Tuite, "The Role of OR in Emergency Evacuation from Hazmat Incidents," Chapter 4, Handbook of Operations Research and Management Sciences Models in Hazardous Materials Transportation, ISBN: TBD, Springer Publishing Inc., New York, anticipated publication in March 2013.

Appendix C-1 - Literature Review - Additional Document Reviews

#1. Framework for Improving Critical Infrastructure Cybersecurity			
Organization	NIST	**Release Date**	February 2014
Type	Framework	**Page Count**	41
Audience	C-level executives, upper- and mid-level operations managers, implementation teams, assessors, consultants, and others interested in understanding the cybersecurity domain		

Content Focus

Applicability

Primary Domains	Stakeholders	Geography	Asset Types
✓ IT ✓ OT	✓ Commercial ✓ Government	✓ U.S. ✓ International	✓ Facilities ✓ Offshore ✓ Vessels

Description

The Framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors. The Core provides detailed guidance for developing individual organizational Profiles. A case-specific Profile is developed by the organization to guide the alignment of its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide an implementable reference model that enables an organization map and measure the relative coverage of its implementation against the cybersecurity Framework. This approach mimics a common closed-loop control system that enables the structured design, implementation, and measurement of a maritime cybersecurity system.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity capabilities sophistication – to uniformly apply risk management principles and best practices to improvement of critical infrastructure security and resilience. The Framework organizes and structures multiple effective cybersecurity standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be applied internationally and serve as a model for international cooperation to strengthen critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, and different risk tolerances. Therefore, how they

implement the practices in the Framework will also vary. The Framework is intended to help better manage cybersecurity risks, optimize security investments, and protect critical services.

Commentary

This document is a result of a presidential Executive Order (EO) to develop a voluntary risk-based cybersecurity framework. While the Framework is described as a set of industry standards and best practices, it is arguably much more. It is an understandable, approachable *reference model* that organizes the highly complex cybersecurity domain in a way that facilitates discussion, establishes design principles, and facilitates security program implementation metrics. The Framework owes much its universal acceptance as a canonical cybersecurity reference document to its structural clarity, domain coverage, real-world usefulness, and support of related national and global standards.

The Framework is designed for use as a strategic reference model, not an implementation model. That is not to say that it cannot be used as an implementation guide – it can. It contains sufficient general cybersecurity implementation content to fill that need. However, its structure and relative simplicity are more suited to other critical purposes. It provides a tractable mental map in its *Core—Tier—Profile* structure that is extremely well suited for:

- Executive understanding of security system design goals/outcomes
- Executive understanding of implementation coverage
- Comparative analysis of a security implementation against a norm
- Implementation baselines that promote and encourage economically and supportable development and progressive improvement
- Preparing an “elevator speech” for when a senior executive asks the cybersecurity program director: “Are we secure or how does our program stack up against the competition?

When used for these purposes, the Framework is remarkably elegant and clear, especially for a 17-page treatment of the cybersecurity domain. But when managers and directors attempt to apply the Framework for detailed implementation, it is less useful because:

- The Framework Core is constructed as a “strategic view”
- The Framework’s “five concurrent and continuous Core Functions” require implementation activities across multiple technical and organizational disciplines, making the structure challenging for work distribution and assessment
- The Framework’s functions, categories and subcategories represent a number of levels of logical implementation abstraction (e.g., PR.PT-2 “removable media is protected” vs. ID.RM-2 “organizational risk tolerance is determined and clearly expressed”) that can undermine implementation and assessment activities

The Framework’s simplicity and clarity is attractive to executives and implementation managers alike; however, implementation managers are cautioned to thoughtfully consider its strategic view, its distribution of technologies and competencies across

all Core Functions, and its presentation of its Functions, Categories, and Subcategories at multiple levels of abstraction before using it as a primary implementation approach. It provides an exceptional strategic reference model, and outlines a useful (and possibly universal) measurement approach to cybersecurity program capability.

#9. The Guidelines on Cyber Security Onboard Ships			
Organization	Baltic and International Maritime Council (BIMCO)	**Release Date**	February 2016
Type	Best Practices	**Page Count**	36
Audience	Ship owners and operators		

Content Focus

Notes: Approximately 10 of the 36 pages are implementable in that they provide a high-level description of generally accepted best practices and recommendations. These descriptions could be used to outline a cybersecurity program or policies. They are not uniformly useful for procedures in that they lack sufficient detail. 13 pages of appendices are provided for additional understanding of the cybersecurity environment, including the NIST Framework.

Applicability

Primary Domains	Stakeholders	Geography	Asset Types
✓ IT ✓ OT	✓ Commercial Government	✓ U.S. ✓ International	Facilities Offshore ✓ Vessels

Description

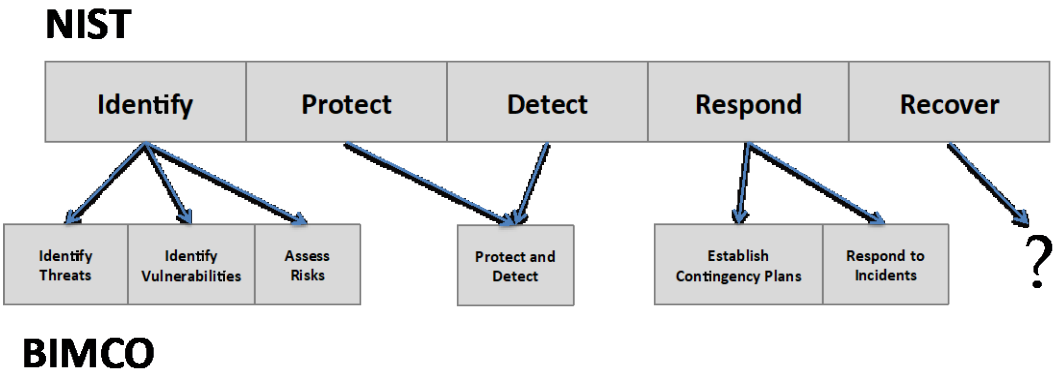
This reference focuses on the unique issues facing the shipping industry onboard ships. The document offers guidance to ship owners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships. That being said the document is not intended to provide a basis for auditing or vetting the individual approach to cyber security taken by companies and ships. The document explores the measures to reduce cyber security risk which include:

- How to raise awareness of the safety, security and commercial risks for shipping companies if no cyber security measures are in place
- How to protect shipboard OT and IT infrastructure and connected equipment
- How to manage users, ensuring appropriate access to necessary information
- How to protect data used onboard ships, according to its level of sensitivity
- How to authorize administrator privileges for users, including during maintenance and support on board or via remote link
- How to protect data being communicated between the ship and the shore side

Commentary

This paper focuses on cybersecurity for cargo and passenger vessels, and therefore limits its cybersecurity discussion to protecting ship handling, cargo management,

and passenger support system as OT systems. The paper presents a graphical model that decomposes and combines the five NIST steps as in the graphic below.



The paper provides a high-level description of its model; however, the content only loosely follows the model as it describes the cybersecurity best practices and recommendations in the text.

#11. Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations			
Organization	ABS	**Release Date**	February 2016
Type	Best Practices	**Page Count**	45
Audience	Maritime and offshore organizations implementing cybersecurity systems on ships, platforms, vessels of any type, and support facilities.		

Content Focus

Note: Primarily useful for incrementally (Basic, Developed, Integrated) establishing a set of IT capabilities needed to support the development of a sophisticated OT security program.

Applicability

Systems	*Stakeholders*	*Geography*	*Asset Types*
✓ IT ✓ OT	✓ Commercial Government	✓ U.S. ✓ International	✓ Facilities ✓ Offshore ✓ Vessels

Description

ABS provides actionable guidance that clearly delineates and differentiates cybersecurity implementation strategies and tactics for IT and OT environments in the maritime and offshore industry. Included are checklists conformant to OT-specific standards and tested on marine and offshore assets to help owners and operators identify gaps in their cyber cybersecurity protections. It also describes a method for evaluating cybersecurity risk management practices that helps owners gauge operational preparedness/readiness with regard to cybersecurity. The availability of actionable

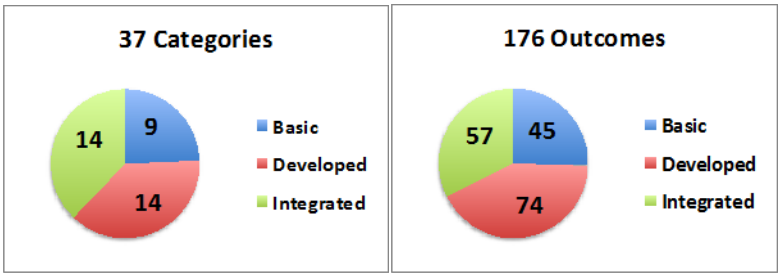
guidance, checklists, and a readiness/capability score described in the ABS guidance provides an owner with a uniform reference by which cybersecurity due diligence can be performed and documented.

Commentary

This document presents a maritime and offshore specific reference model for establishing organizational cybersecurity capabilities. Key content within the reference include:

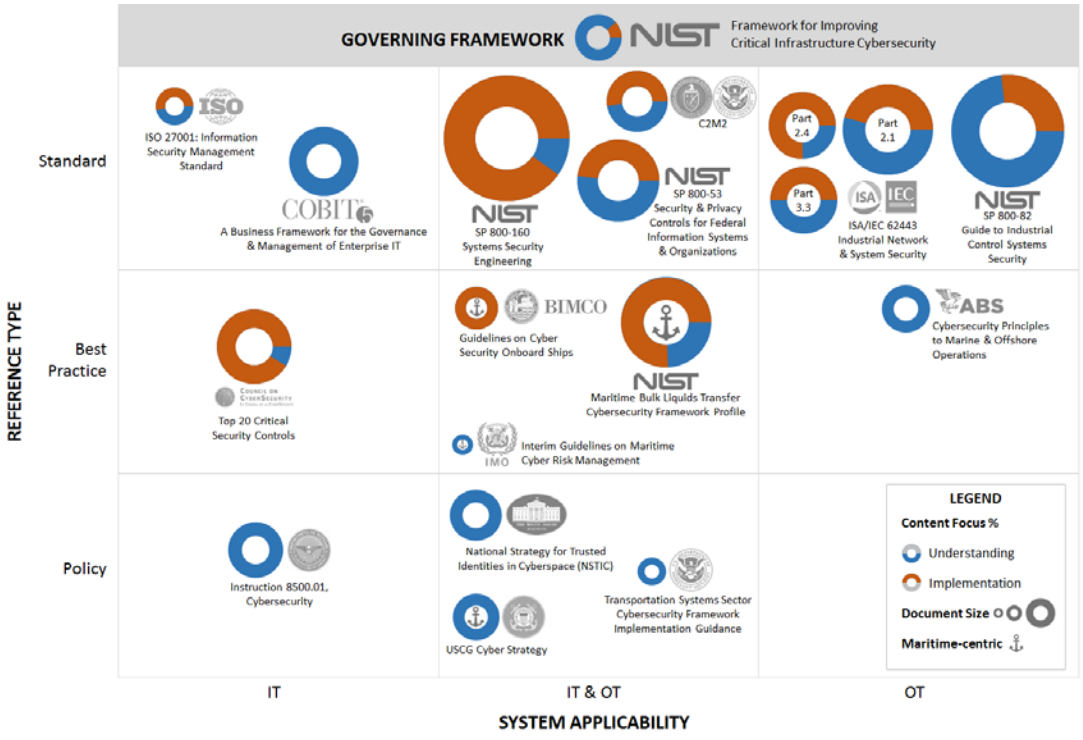
- Extended definitions of high-level terms often used in cybersecurity discussions, including definitions of IT, OT, and smart assets.
- The structure of the ABS cybersafety set of guidance documents.
- A graphical (page 7) and descriptive model for progressive organizational development of cybersecurity capabilities: basic (9 categories), developed (14 categories), and integrated (14 categories).
- Page 9, 17 pages: Basic capabilities are listed and illuminated by key cybersecurity capabilities and/or behaviors that characterize an organization that is beginning to implement security protections.
- Page 17, 11 pages: Developed capabilities are listed and illuminated by key cybersecurity capabilities and/or behaviors that characterize an organization that has developed a fully operational security system and support team.
- Page 28, 12 pages: Integrated Capabilities are listed and illuminated by key cybersecurity capabilities and/or behaviors that characterize an organization that has linked it security protection systems throughout the organization as part of the corporate culture, and includes proactive protective analytics and management procedures.

Each capability category is followed by a set of 5-10 implementation outcomes. The outcomes are useful examples of protective processes from which security policies may be developed. The outcomes under each capability category are following by an instructive explanation of the purpose behind the outcomes, and references for additional explanation. It is a scholarly paper useful for both IT and OT environments.

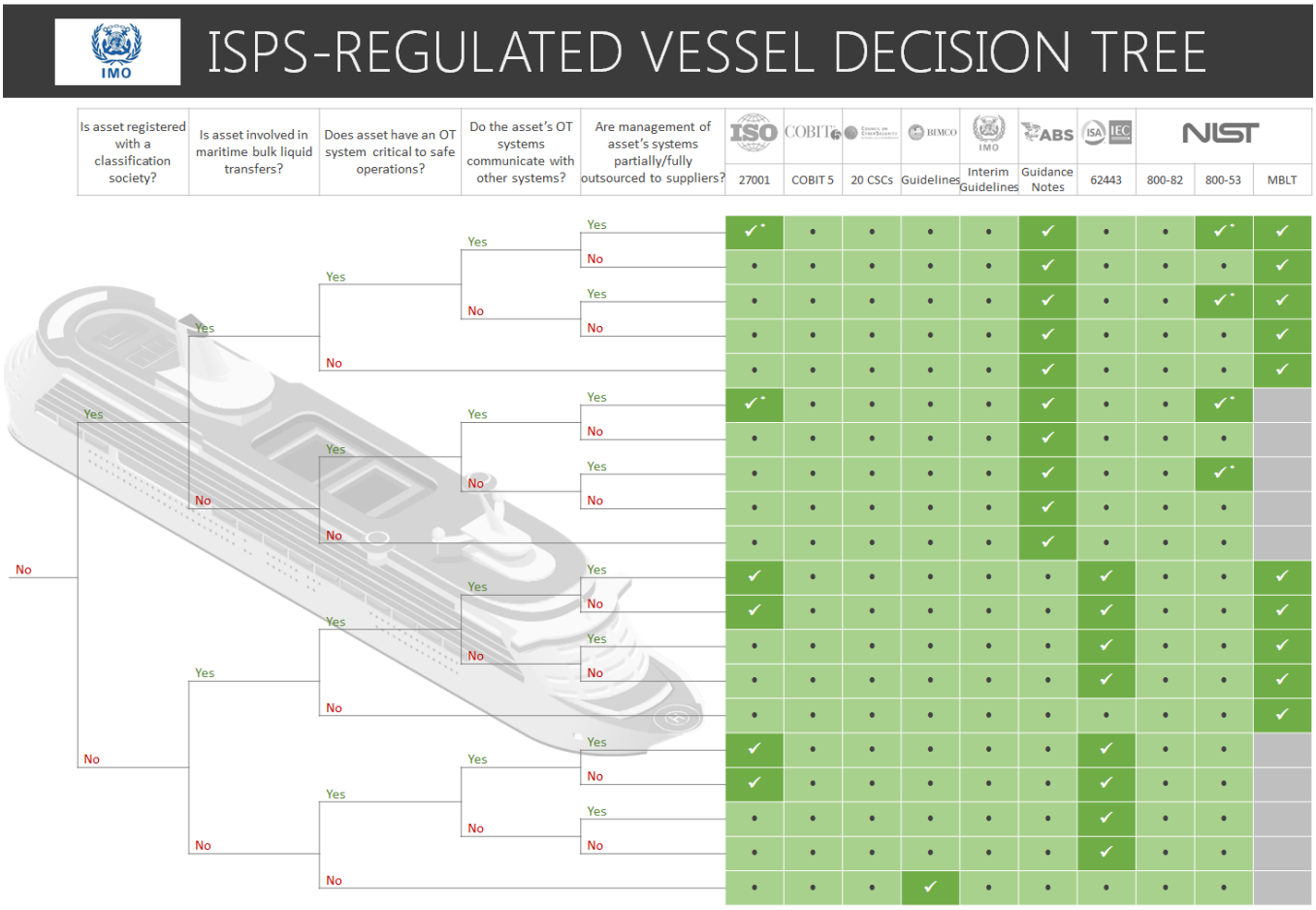


Appendix C-2 - Literature Review Summary

The graphic below summarizes the literature review described earlier in Table 4, where each reference is plotted on a matrix indicating its type (policy, best practice, standard, or framework) vs. its applicability to IT, OT, or both. The size of each reference's donut chart indicates its page count and the color indicates the reference's percentage focus on implementation (orange) vs. understanding (blue). References that explicitly address maritime issues are identified with an anchor icon.



Appendix C-3 - Decision Tree Example: ISPS- Regulated Vessel



Appendix C-4 - Point of Failure Detection Framework Worksheet (Drill Ship or MODU)

Virtual Asset Depth	Cybersecurity Attributes: Virtual Asset Breadth		Select Only One	Asset Functions: 1 Electronic Chart Display	2 Radars	3 GPS	4 INMARSAT-C	5 Navigation lights	6 Signal Light Column	7 Navigation Automations	8 Bridge Control Console	9 Machinery Control	10 Automated Identification	11 Gyro	12 Fleet Broadband	13 VHF Radiotelephone	14 MF/HF Radiotelephone	15 Voyage Data Recorder	16 Engine Control Room Console	17 Main Switchboard	18 Ride Control	19 Generators	20 Steering Stand	21 Propulsion	22 Thruster Control	23 Burner Control	24 Propulsion Alarms	25 Ballast Control	26 HVAC	27 Drilling & Well Control	28 Emergency Shutdown	Criteria
Cyber Complexity Attributes *check box if yes*	1	This function is deployed on one or more assets within the enterprise																														One or multiple instances of this function are installed in the fleet. Please estimate number of instances.
	2	This function is critical to safe operation																														Reduced performance of this function can hazard human life, the asset, or the environment.
	3	This function's control connection is "Discrete	Select Only One																													**1:1** Equipment is linked to its control connection only
		This function's control connection is "Simple"																														**1:Few** Equipment is linked to multiple other control connections directly (without a network)
		This function's control connection is "Complex"																														**1:Many** Equipment is linked to multiple on-asset control connections through a network
		This function's control connection is "VLN"																														**1:Very Large Number (VLN)** Equipment is linked to the Internet
	4	This function is managed by the equipment and/or control system provider																														Equipment supplier provides "turn-key" support to the equipment, including security support
	5	This function does not have supplier-provided control system documentation																														Equipment supplier does not provide a detailed Functional Description Document (FDD) to the owner/operator
	6	This function's control system is protected by the system supplier's cybersecurity system																														Equipment supplier provides cybersecurity monitoring and protection for the function's control system

Virtual Asset Depth		Cybersecurity Attributes		Criteria
Business Attributes *check box if yes*	1	The asset is not MTSA-regulated.		Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.
	2	The asset is not registered with a classification society that has cybersecurity guidance		Classification society "rules" are not implemented or required of a cybersecurity implementation.
	3	Land-based IT or OT systems communicate to the asset's OT systems		Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.
	4	Each asset is uniquely equipped		OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.
	5	The company has not developed policy governing IT cybersecurity		IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available
	6	The company has not developed policy governing OT cybersecurity		OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available
	7	OT cybersecurity is provided by a 3rd-party supplier		A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protections.
Cybersecurity Documentation Attributes *check box if yes*	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented		An office/individual responsible for security of IT systems has not been established
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented		An office/individual responsible for security of OT systems has not been established
	3	Incident Response Team (IRT) responsibilities are not documented		An office/individual responsible for supervising the response to security incidents related to OT systems has not been established
	4	An OT FDD has not been developed		A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset-specific design schematic.
	5	A compiled cybersecurity FDD is not available		The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset-specific design schematic
	6	Management of Change (MoC) documents are not available		Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC documentation.
	7	Cybersecurity training documents are not available		Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.

APPENDIX E-1 SRI 2017 Student Survey

MARITIME SECURITY CENTER

SRI 2017 Student Survey

1. Student Survey

This survey is designed to document the SRI's impacts on your knowledge and understanding of Maritime Security tools, technologies and applications, and the challenges faced by the Department of Homeland Security in securing the Nation's ports, inland waterways, and coastal borders. We also want to assess the quality of the SRI program from your perspective.

Please take the time to provide us with as much detailed information as possible in the open-ended questions of this survey.

We thank you for your time and feedback!

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

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

*** 2. How would you describe your knowledge of maritime security tools and technologies (e.g. ROVs, acoustic systems, etc.) prior to the SRI?**

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

*** 3. How has your knowledge of your assigned research area (e.g., Maritime Cybersecurity, Arctic Acoustics, VR and ROVs) improved over the course of the eight-week summer research program?**

	1=Did not Improve at all	2=Improved (I have a basic understanding of the concepts.)	3=Improved Sufficiently (I can effectively apply my knowledge.)	4=Improved Substantially (I have gained advanced knowledge and confidence in this area.)
Knowledge of research project area.				

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

	1=Not at all	2=Somewhat (Very little improvement in this area.)	3=Improved Sufficiently (My skills have improved and I can effectively apply what I have learned.)	4=Significantly Improved (I have significantly improved my skills and I feel confident in my capabilities in this area.)
Ability to Conduct Research	○			
Communication Skills				
Leadership Skills	○			
Networking				
Oral Presentations				
Professional Confidence				
Teamwork/Collaboration				

Other (please specify)

*** 5. In your opinion which of the skills above did you improve the most and what activities in the SRI helped you improve these skills?**

6. What skills would you have liked to improve more? (e.g., presentation skills, report writing, networking, etc.)

*** 7. Rate the SRI with regards to the following items:**

	1= Not good at all	2= Good	3= Very Good	4= Excellent
Quality of Program Coordination/Administration				
Faculty Mentor Guidance and Assistance				
Quality of the Program Curriculum				
Quality of Faculty Lectures				
Quality of Guest Lectures				
Quality of Teamwork				
Quality of Field-visits				
Quality of Research Facilities				
Quality of Research Outcomes				
Ability to be Innovative and Self Motivated				

*** 8. What are your top 3 takeaways from this summer's program? (We would like to quote your responses, so please provide as much detail as possible.)**

*** 9. What would you say are the strengths of the SRI? (e.g. Administration, Faculty interaction/collaboration, Student team work/collaboration, Research assets, Field-visits, Experiments, Networking opportunities, etc.) Please provide as much detail as possible.)**

*** 10. What can the Maritime Security Center do to improve the Summer Research Institute for future student groups? (Please provide as much detail as possible.)**

*** 11. How would you best describe your experience in the SRI?**

*** 12. What topics, lectures, and/or field visits did you find most interesting and engaging?**

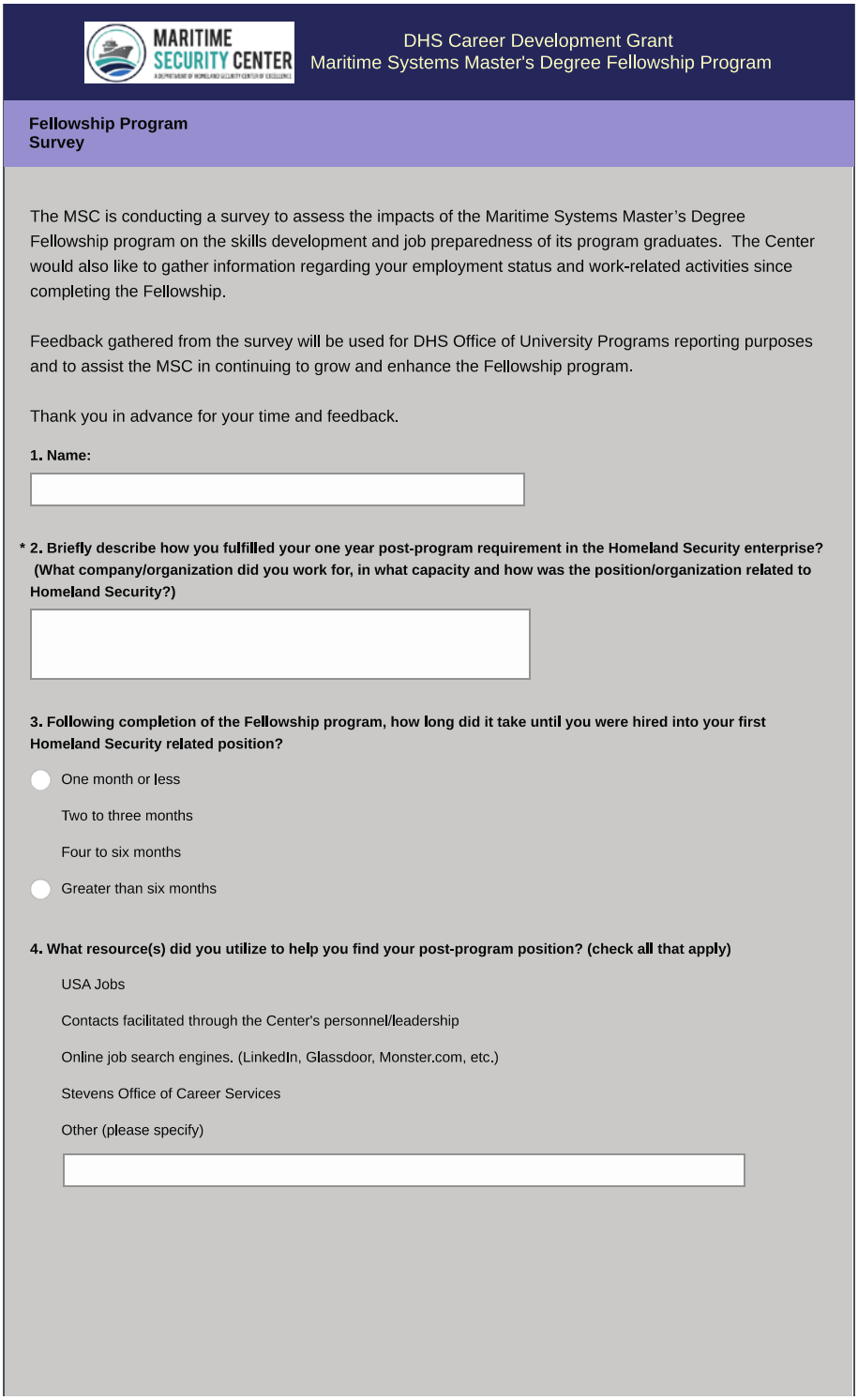
*** 13. Has the SRI enhanced your interest in pursuing a career and/or further academic study in the field of maritime/homeland security?**

- Yes
- No

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

- Yes
- No

APPENDIX E-2 Fellowship Alumni Survey



MARITIME SECURITY CENTER

DHS Career Development Grant
Maritime Systems Master's Degree Fellowship Program

Fellowship Program Survey

The MSC is conducting a survey to assess the impacts of the Maritime Systems Master's Degree Fellowship program on the skills development and job preparedness of its program graduates. The Center would also like to gather information regarding your employment status and work-related activities since completing the Fellowship.

Feedback gathered from the survey will be used for DHS Office of University Programs reporting purposes and to assist the MSC in continuing to grow and enhance the Fellowship program.

Thank you in advance for your time and feedback.

1. Name:

*** 2. Briefly describe how you fulfilled your one year post-program requirement in the Homeland Security enterprise? (What company/organization did you work for, in what capacity and how was the position/organization related to Homeland Security?)**

3. Following completion of the Fellowship program, how long did it take until you were hired into your first Homeland Security related position?

- One month or less
- Two to three months
- Four to six months
- Greater than six months

4. What resource(s) did you utilize to help you find your post-program position? (check all that apply)

- USA Jobs
- Contacts facilitated through the Center's personnel/leadership
- Online job search engines. (LinkedIn, Glassdoor, Monster.com, etc.)
- Stevens Office of Career Services
- Other (please specify)

*** 5. How would you best describe your one year post-program Homeland Security employment experience? (check all that apply)**

- [ ] The position/organization was a good match for my educational background.
- [ ] The position utilized the skills I developed in the Fellowship program.
- [ ] I was well-prepared for the job responsibilities.
- [ ] The position and organization were not a good fit for me.
- [ ] The Fellowship program did not adequately prepare me for my post-program Homeland Security employment.
- [ ] Other (if none of the above apply, please describe your experience)

6. What is your current employment status?

- [ ] I am still employed by the organization I worked for following the Fellowship program.
- [ ] I am employed in the workforce.
- [ ] Attending graduate school fulltime. (PhD program)
- [ ] Currently unemployed and not attending college (If you checked this box, please skip to question 11.)

Other (please describe your current status if none of the above apply)

7. If you are employed, who is your current employer?

8. What is your position title?

9. How would you best describe your primary job responsibilities?

- [ ] Technical
- [ ] Administrative
- [ ] Consultant/Analytic
- [ ] Other (please describe)

10. Is your current occupation related to homeland security operations or in support of homeland security missions?

- [ ] Yes
- [ ] No

If Yes, how so?

*** 11. What skills/knowledge did you develop in the Fellowship program that have been most useful to you in your employment? (check all that apply)**

- [ ] Technical knowledge (sensors, sensor applications, MDA, engineering concepts, etc.)
- [ ] Ability to analyze and assess complex issues/problems.
- [ ] Ability to orally present concepts, ideas and information.
- [ ] Ability to prepare written reports and analysis.
- [ ] Ability to conduct independent research.
- [ ] Team work/collaboration.
- [ ] I did not learn any of the above skills in the Fellowship program.

Other/Additional Skills. (please describe)

*** 12. What aspects of the Fellowship program do you feel had the most impact on your professional development? (check all that apply)**

- [ ] Graduate coursework.
- [ ] Thesis research.
- [ ] Field-based internship.
- [ ] Faculty mentorship.
- [ ] Inclusion in Center meetings and interactions with practitioners.
- [ ] Other (please specify)

*** 13. How would you rate your skills and knowledge compared to those of your colleagues in the same capacity?**

- [ ] The Fellowship program provided me with more technical knowledge, skills and experience than my counterparts.
- [ ] We are equally educated and capable.
- [ ] My colleagues possess greater technical depth and knowledge.

Comments:

14. As you reflect on your participation in the Fellowship program, is there any way the Center could have been more effective in preparing you for your post-program experience? (e.g.,more/less faculty engagement, more/less assistance with job placement, provide a different sequence of course offerings, or more rigorous courses, etc.)

15. We welcome any additional comments you might have about your experience in the Fellowship program. (optional)