THE PATHWAY TO ACCREDITATION: "DOMAIN" Deliverables (and Benefits) in each part of the ADaPt Process

Although some ports may have many of the DOMAIN elements already in place and can go right to the Accreditation phase, many ports do not have all the ingredients. This portion of the proposal outlines how we can assist **A port** to "**ADaPt,**" with "best-in-class" tools and processes in order to achieve that Accreditation status. The following section breaks down each **DOMAIN** element and outlines the deliverable for each part of the process.

1.0 DIGITIZATION

A "Smart Port" has been defined as one that uses automation, and innovative technologies such as Artificial Intelligence (AI), Modeling and Simulation, and the Internet of Things (IoT) to enhance operational performance. Digitization is the next step where technology is allowed to be the baseline that supports innovation. The first and most fundamental component of MARSEC Accreditation is to establish a Digital Twin.

A Digital Twin is a virtual representation of the physical site and facilities (critical infrastructure) that are being protected at **A port**. The Digital Twin is a 3D, digital model that consists of terrain features and the major elements that impact line of site and movement in the port including structures, major equipment and objects.

The ARES Digital Twin includes details about a site's guard force, security CONOPS, and security technologies such as sensors and cameras, perimeter structures, and barriers. 'Digital Twin' data offers owners of maritime critical infrastructure an opportunity to identify, monitor, analyze and optimize both operational and security requirements. This baseline tool provides verified and organized datasets that can be used to support various requirements (Vulnerability Assessments, Training & Exercises) in other components of MARSEC Accreditation. The Twin provides ports with a critical component that will directly impact preparedness, readiness, responsiveness and resiliency.

1.1 DIGITAL TWIN Value Proposition

- ✓ The ARES Digital Twin is immediately available to support Vulnerability Assessment requirements, such as the MTSA Facility Security Assessment, as well as many other additional applications. The ARES Digital Twin becomes an asset that makes future assessments or analyses much more efficient, by eliminating the need to re-baseline. The Digital Twin is refreshed annually, as part of the service, and assessments do not need to be start with a site survey. Additionally, **A port** can use the Digital Twin continually to perform quick cost/benefit analyses, or full-on assessments to thoroughly analyze new threats or proposed security design changes.

  Cost savings: Future Analyses and Assessments less expensive

- ✓ The Digital Twin, and associated AVERT® simulations, can be uploaded into AVERT® Virtual Tabletop to facilitate exercises. This capability removes the guesswork associated with traditional training exercises, and tabletop drills, and can provide realistic training scenarios that have already been simulated using AVERT® Physical Security. In AVERT® Virtual Tabletop, users can be prompted to make decisions based on the previous AVERT® Physical Security analysis, and can view and evaluate the outcome of those decisions in real time.

  Cost savings: Virtual Tabletop Training can replace some physical training

1.2 DIGITAL TWIN Scope of Work & Deliverables

ARES will work with **A port** to access certain data elements that support development of the Digital Twin. If some/all of these data elements can be provided directly to ARES, time required to develop the Twin will be reduced. If certain data are not available, the ARES PM will work with the Port to develop a plan to capture the missing items in the most expeditious and cost-effective way. The accuracy and classification of the Digital Twin are a fundamental, pre-requisite component of the AVERT® simulations, that also support MARSEC Accreditation. Data input to develop the Digital Twin:

- ☐ Large Scale Topographic GIS Maps (including attributes and heights of features) in an ESRI Geodatabase format. This database needs to include:
  - Planimetric Features such as Roads, Fences, Barriers, Structures such as Buildings, Shoreline, Driveways, Parking, Landing Areas, Access Control Points, Quay Walls, Boat Ramps…etc.
  - Major Permanent Equipment affecting the Line of Sight
- ☐ Ortho Imagery in a GeoTIFF format
- ☐ Digital Elevation Models (DEM) in a GeoTIFF or Geodatabase format
- ☐ Barriers and Access Control Location and Composition
- ☐ Security Technology Specifications and Locations such as cameras, lighting, IR, barriers, etc
- ☐ Guards and Security related information such as equipment, patrol routes, comms, etc.

In the event the Port does not have access to the GIS databases, ARES would require existing drawings (Paper or CAD Data). ARES will digitize paper drawings to be included in the Digital Twin.

Attention to detail is essential, during development of the Digital Twin, as it directly impacts the accuracy of any subsequent security analysis. ARES will need to have physical access to the Port to

perform a Site Survey to verify/supplement information such as sensor locations, new construction, etc. Additionally, surveyors will spot check to identify any information that could be out of date or inconsistent with the GIS inputs. The site survey will also focus on verifying the security-related input relative to guards, equipment, patrol routes, etc.

ARES Security will provide secure, encrypted storage for all Digital Twins. If desired, ARES Security will facilitate Digital Twin data sharing opportunities, with the U.S. Coast Guard, to be directed by individual Ports.

☐ **Deliverables**

a.) Digital Twin in COLLADA format + secure storage

b.) Training (2 hours) to familiarize users with the Digital Twin and related applications

c.) Annual refresh to verify/validate Digital Twin baseline

2.0 OPTIMIZATION: Assessments, Training & Exercises

Vulnerability Assessments provide the foundation for the effective implementation of maritime security measures at ports and port facilities. Every one of Americas 300+ ports are different, with different security infrastructure, and different risk profiles. Vulnerability Assessments can be both expensive and subjective, based on who is performing them. To support MARSEC Accreditation, ARES Automated Vulnerability Evaluation for Risks of Terrorism (AVERT®) software portfolio provides a tool to reduce cost associated with Facility Security Assessments and Facility Security Plans. Applying the AVERT® software to this challenge will provide **A port** with an opportunity to reduce cost, eliminate variability in analysis and output, optimize results related to risk analysis, and standardize the vulnerability assessment process and eliminate subjective input.

AVERT® risk assessment software works in tandem with the Digital Twin to enable experts to visualize, quantify, assess and optimize the security posture at a designated site. AVERT® delivers an accurate, measurable, and repeatable decision support tool to optimize the physical security analysis process.

Developed by ARES Security Corp, AVERT® provides unique modeling and simulation software that visualizes security performance and quantifies risk profiles and response configurations. These outputs will provide **A port** with a detailed understanding of their comprehensive security and response configuration's effectiveness. Whether performing a cost-benefit analysis on security systems, or a comprehensive vulnerability analysis, the AVERT® solutions have saved clients millions of dollars while increasing their security effectiveness. AVERT® software has been accredited by the Department of Defense and the Department of Energy, certified by the Department of Homeland Security, and published as a “Best Practice” by the World Institute of Nuclear Security.

As a starting point toward MARSEC Accreditation, AVERT® is used as a tool to support the MTSA Facility Security Assessment requirements. With the AVERT® Physical Security solution, **A port** can comprehensively evaluate any existing or planned security systems including cameras, perimeter intrusion detection sensors, alarms, access control systems, barriers, and many others to determine optimum security employment and cost effectiveness. By establishing a security enterprise baseline, in the Digital Twin, **A port** can use the AVERT® software to perform quantitative analysis of their security

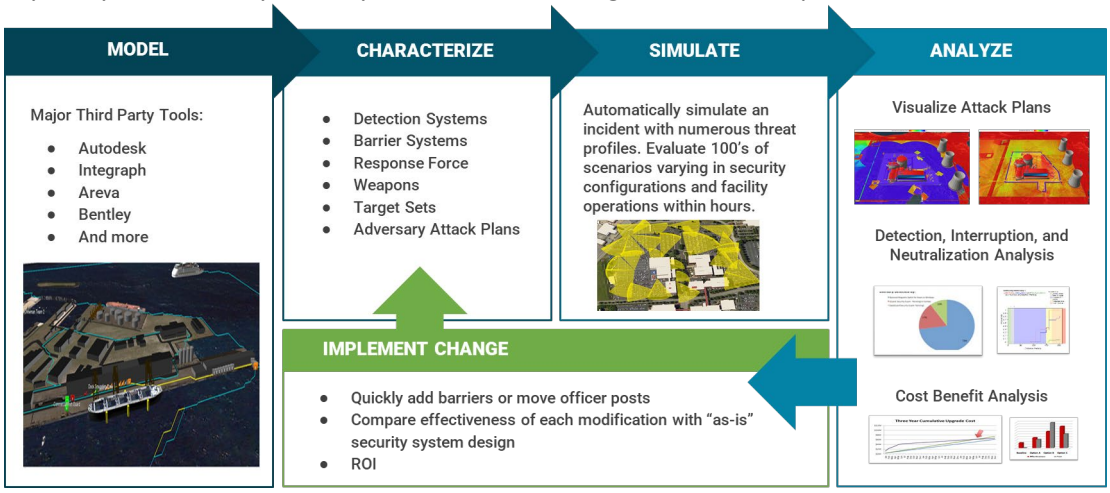
posture, using whatever Design Basis Threat is appropriate. The software will identify security gaps, as well as rate the effectiveness of the current security posture. This analysis is not subjective, but rather determined by algorithms and security data libraries that have been independently vetted and approved by the U.S. Departments of Defense and Energy.

2.1 ARES AVERT® Value Proposition

The benefits from utilizing this powerful decision support tool include:

- ✓ Provides an effective, quantifiable system for evaluating the entire facility security posture rather than security component level assessment.
- ✓ Reduces reliance on subjective judgement of SME's and over reliance on security component design specifications.
- ✓ Quantifies security risks, expenditures, and benefits.
- ✓ Uses simulation to evaluate permutations of security design (i.e., location of and number of security devices) to achieve desired performance outcomes.
- ✓ Provides process to evaluate alternative security detection and deterrence strategies / technologies that were previously unidentified.
- ✓ Identifies vulnerabilities and validates changes to security detection / deterrence strategies and technologies, the number of Security personnel required to delay and neutralize an adversary, the impact of critical detection and delay systems and firepower required to thwart an attack, and more.
- ✓ Analyzes thousands of threat scenarios and response permutations to determine Security Effectiveness.
- ✓ Identifies security cost savings through quantified risk assessments and cost benefit analysis. Current ARES Security customers have reduced security costs in some instances by as much as 50%, saving users tens of millions of dollars.

AVERT® uses an advanced modeling and simulation engine to quickly perform defense-in-depth and sensitivity analysis to identify security vulnerabilities, mitigate risks, and optimize cost.



Once **A port** has a Digital Twin, the AVERT® decision support tools bring an intuitive user interface that uses the realistic 3D models of the port including access points and entrances, natural features, and the placement of security technology (cameras, barriers, radars, etc.) to facilitate analysis.

Cost savings: Facility does not have to be physically surveyed every time an FSA is done.

AVERT® uses Monte Carlo simulations in order to evaluate security vulnerabilities. An exclusive pathing algorithm determines the various potential vulnerabilities that could be exploited. AVERT® output will provide **A port** with a complete understanding of the existing security posture, with regard to addressing vulnerabilities, and options to optimize the security solution for both effectiveness, and costs.

Cost savings: Security recommendations are optimized for cost/benefit.

The analysis parameters in AVERT® can be easily changed within the model to address a wide range of security system configurations, threats profiles, and risk elements. Once the vulnerabilities and pathways have been identified and analyzed, users can adjust, test, and evaluate various notional security solutions (sensors, systems, and procedures) by testing their effectiveness in the software. An unlimited number of iterations can be considered in this process. AVERT® output will provide **A port** with a detailed analysis of security effectiveness, and thorough cost/benefit analysis, that is calculated using algorithms, and data libraries, that have been independently validated by the U.S. Departments of Defense and Energy.

Cost savings: security solutions can be tested/verified virtually using software.

This quantitative approach to risk management also offers **A port** a cost-effective means to continually assess risks and optimize security effectiveness. Rather than only assessing facility security requirements once every 3 to 5 years, the AVERT® software can analyze on an ongoing basis as security upgrades are made, and as the threat profile changes.

Cost savings: security posture can be analyzed continually with no additional investment.

2.2 ARES AVERT® Scope of Work & Deliverables

ARES will ensure access to AVERT® Physical Security Software as a Service (SaaS). **A port** will have a web-based, state-of-the-market decision support tool that optimizes development of Facility Security Assessments, and Facility Security Plans as well as virtual tabletop training.

AVERT® Physical Security can be used to support **A port** security team by digitally addressing important questions that can have a significant impact on overall security effectiveness, such as:

- Are there any gaps in coverage that could affect overall security effectiveness?
- What are the costs vs. benefits of the various security technology options?
- How will the current security strategy work against various threats?
- What improvements can be made to increase security effectiveness?

Answering these questions usually requires additional resources beyond the best judgement of a Subject Matter Expert. Comprehensive answers to these complex and critical questions can often only be determined through quantitative analysis, using software (decision support tools). The AVERT® Physical Security solution was designed and built by ARES Security to answer these complex questions.

☐ Design Basis Threat

ARES Security will provide oversight and guidance, within the SME hours proposed, to work with **A port** personnel, including designated consultants, to develop a list of up to 10 target sets that will be used for the Vulnerability Analysis. The CARVER and Adversary Mission Analysis (AMA) methodologies, as well as others, may be used in this process. The objective will be for **A Port** to identify a realistic set of threat scenarios (Design Basis Threat), that will be used by the AVERT® software for analysis. Personnel designated by **A Port**, will utilize the US Department of Homeland Security data, as well as **A Port's** data, and the ARES Digital Twin, analyze port security posture versus potential targets and threats. A variety of simulations and pathway analyses can be run in the software using the designated threat scenarios and targets.

☐ Vulnerability Analysis

The AVERT® SaaS license includes ARES Subject Matter Expert (SME) oversight and guidance for vulnerability analysis work necessary to meet MTSA Facility Security Assessment requirements. ARES agrees to provide up to (24 hours per year) of SME support for this assessment work. The AVERT® 4 step process is outlined below:

TASK 1: CHARACTERIZE. Details each security element are accounted for based upon detailed performance data from the AVERT® Library, which contains data on most security systems, platforms, weapons, detection, and delay systems. SMEs contribute data about guards, law enforcement responders and their level of proficiency. The site's security plan is also added to the system and includes target sets, adversary attack plans, tactics, and objectives.

TASK 2: SIMULATE. AVERT® runs a comprehensive analysis to identify the best path for each adversary to access the facility or site based on their objective. The software then runs exhaustive simulated attacks for each of these vulnerabilities to determine overall security effectiveness.

TASK 3: ANALYZE. Visualizations, charts, graphs, and metrics are produced to give users insight into the effectiveness of the current security posture. These powerful reports clearly and objectively identify gaps and evaluate potential upgrades or modifications.

TASK 4: OPTIMIZE. Users can optimize their overall physical security system configuration and procedures, using the AVERT® Physical Security assessment, by evaluating a virtually unlimited number of tactics and security system configurations, and comparing security effectiveness against an established Design Basis Threat.

☐ Deliverables

a.) Software as a Service license (1 year) to AVERT® Physical Security and Virtual Tabletop

b.) Training (24 hours) to familiarize expert users with AVERT® software

c.) SME Support (24 hours) (remote) for Vulnerability Assessment support

d.) Help Desk Support

3.0 MATURITY: Cybersecurity

Because cyber risk is a persistent, ever-evolving danger to port and maritime operators, effective cyber risk management cannot be achieved through an annual checklist-based approach. Therefore, this element of the MARSEC Accreditation program offers a maturity model methodology to support **A Port** as it aligns with established best practices, nationally recognized standards, and federal/international guidelines for cybersecurity.

To successfully address the complexities of today's cyber threat environment, effective cyber risk management requires both persistent engagement, and a multi-disciplined approach. Managing cyber risk is not just the responsibility of the IT department. This element of the program must facilitate a shared obligation among all key stakeholders and include them in the maturity assessment process - security, operations, health and safety, administration, finance, accounting, incident response, training, legal, communications, and procurement.

PortLogix, developed by HudsonCyber and recognized by Lloyd's as a Digital Innovation Winner, was selected to provide an organizational "starting point" for assessing cybersecurity. PortLogix is not a scanning tool, monitoring application, or form of network defense. It is a cloud-based application that brings together stakeholders from across the organization to stimulate in-person (or virtual) cross-functional collaboration, promote awareness, and enhance communication and information sharing. It facilitates self-assessments that baseline, target, measure, and support cybersecurity capability growth and cybersecurity resilience over time.

In January 2020, the United States Coast Guard issued Navigation and Vessel Inspection Circular (NVIC) No. 01-2: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA). This circular outlined the requirements for assessing and addressing computer system or network vulnerabilities. Specifically, USCG reaffirmed that under the current regulations facility owners and operators must identify and analyze vulnerabilities related to their radio and telecommunication equipment, including computer systems and networks. Facility owners and operators are required to include any identified vulnerabilities, called cybersecurity vulnerabilities, in their Facility Security Assessments and then address those cybersecurity vulnerabilities in their Facility Security Plans.

To support these requirements, Hudson's cybersecurity decision support tool has been designed to help **A Port** achieve two high-level objectives:

a.) Implement the PortLogix® cybersecurity program across **A Port**'s operating environment

b.) Engage with stakeholders through a blend of training, virtual collaboration and onsite professional services, to evaluate and manage cybersecurity maturity at **A Port**

3.1 PortLogix® Value Proposition

Engagement through PortLogix® institutionalizes cybersecurity processes and procedures, and informs the sustainable allocation of resources (i.e., people, processes, tools, and funding), by providing **A Port**'s leadership with the ability to:

- ✓ Assess cybersecurity capabilities across TPA's facilities.
- ✓ Measure, monitor, and benchmark cybersecurity improvements.
- ✓ Coordinate and efficiently allocate resources (people, processes, tools, and funding), and save money.
- ✓ Enable continuous assessment, monitoring, and improvement.
- ✓ Inform risk transfer (insurance) determinations.
- ✓ Drive collaboration during the assessment process and the implementation of mitigation measures that support capacity development.
- ✓ Empower and educate staff through hands-on analysis.
- ✓ Assist stakeholders in developing cybersecurity target profiles.
- ✓ Foster a cyber-aware culture through consensus-based analysis and assessment.
- ✓ Support investment planning and prioritization activities.
- ✓ Standardize cybersecurity performance metrics across all TPA assets.
- ✓ Streamline and standardize internal audit and inspection activities.
- ✓ Be able to initiate assessments and teams in minutes.
- ✓ Benchmark internal growth and compare progress against industry peers.

3.2 HudsonCyber – PortLogix Scope of Work & Deliverables

PortLogix® will facilitate cross-functional collaboration at **A Port** by engaging stakeholders across twelve primary functional areas: Cyber Risk Management, Cyber Program Management, Information & Communication Technologies, Commercial & Supply Chain Practices, Governance, Workforce Management and Training, Change Management, Situational Awareness, Information Sharing, Threat and Vulnerability Management, Physical Security, and Incident Response & Business Continuity.

a.) Software as a Service license (1 year) to PortLogix®

b.) Training (16 hours) to familiarize expert users with PortLogix® software

c.) Compliance Map for PortLogix® content

d.) PortLogix® Reports

e.) Help Desk Support

4.0 ACADEMIC ADVANCEMENT

As described in a White Paper published in 2017 titled *Navigating the Changing Seascape in Maritime Public Safety,*[1] and again reiterated in multiple conference presentations throughout the last few years (see "Transforming Training after the Storm" presentation at CALEA Conference and "Training the Maritime Workforce" - an IBEX Workshop[2]) the maritime industry as a whole is facing the "Perfect Storm". With retention issues mounting, diversity challenges continuing, and recruitment opportunities dwindling while organizations lose their institutional knowledge through increasing retirements, the "wave" of the Perfect Storm hit us well before the pandemic. Now, the dynamic changes in our workforce have required us to change how we operate – but more importantly – how we train.

Building off of the training capabilities built into and part of the ARES AVERT software, and the HudsonCyber PortLogix program described in detail earlier in this document, the NMLEA will utilize its extensive experience in training, adult-learning, and instructional design to provide these tools and resources to **A Port** in order to foster and facilitate true workforce development:

☐ **Required MTSA Training – now available through *PortTraining***

The NMLEA's online MTSA Training portal - **PortTraining**[3], is the nation's only comprehensive seaport security curriculum with flexible delivery options and online training management. With Department of Homeland Security funding and direct oversight by the US Coast Guard, the US Maritime Administration, and FEMA, a team of 72 Florida State University instructional designers and staff developed this single-point training solution for ports, terminal operators, and first responder agencies. An active Industry Advisory Group guided every phase of work with the goal of creating a whole-system approach that "meets regulatory requirements...while recognizing seaports' central purpose of commerce."

The DHS/FSU partnership designed **PortTraining** to be the next generation in security training. Two innovations stand out for their significant implications: (1) the introduction of Web-based training for MTSA required training with flexible delivery options and lower costs, and (2) the online management of all training records. Four courses with 480 lessons fulfill Coast Guard and MARAD requirements, but they go far beyond requirements, providing 24/7 professional development opportunities.

The cost-savings of the **PortTraining** approach versus purely instructor-led training are significant, primarily because of the additional web-based delivery option. And the savings grow with the size of the facility or, in the case of large companies with distributed operations, with the number of terminals. **PortTraining** courses ensure regulatory compliance, and the secure training management system can be integrated with an existing HR system for true enterprise management of security training.

[1] https://www.nmlea.org/research-and-white-papers: *Navigating the Changing Seascape of Maritime Public Safety*

[2] https://www.nmlea.org/webinars-and-podcasts

[3] https://www.nmlea.org/porttraining

A Port would join ports like Canaveral[4], Alabama[5], Houston[6] (see below for links) and others in this PortTraining online community, with customized/branded educational portals.

☐ **Beyond PortTraining: Making all training more affordable, more accessible, more adaptable, and more advanced with *aLEX*.**

Since its inception in 2000 under the leadership of ADM Siler (former USCG Commandant), the NMLEA has been an institution with no walls, exporting all of its instructor-led training to the bays, rivers, lakes, harbors, and coastline of the United States (and internationally), so that agencies and public safety professionals can receive their training in their area of operations, in their ports, on their boats, and alongside their local partners. Understanding the increased challenges to time, budgets, and an evolving workforce that public safety agencies are facing all across the country, the Academy has used its knowledge, relationships, resources, adult learning expertise, and technology partnerships to expand on virtual training and provide a mobile, easily accessible and affordable solution for every officer and department.

Called **aLEX[7],** the AcademyOnline Program provides a wealth of online learning tools that allow you, to transform your traditional Instructor-Led Training (ILT) into an adaptable, affordable, accessible mobile learning platform. Put simply, we can take any training you do now, and transform it into a digital journey for your people.[8]

Customized and branded to **A Port**, there is no research that has to be done on what LMS to purchase, or time spent searching for a platform to use to record your teaching, track your people and document what they've learned, how they learned and when they learned. There is no learning-curve or struggle trying to figure out how to translate a traditional Instructor-Led Training (ILT) course into the online environment. The Academy staff will work with you and facilitate the process.

☐ **Degree Programs and Continuing Education Credits from the University of South Florida**

The mission of the Center for Maritime and Port Studies (CMPS) at the University of South Florida (USF), is to address the needs of the coastal community stakeholders by (1) providing on-line education, training, and continuing professional development for careers in the maritime transportation industry; (2) conducting research on security, sustainability, and resilience of the maritime transportation system and related activities; and (3) providing rigorous, independent testing and evaluation of maritime

[4] https://canaveral.port.training/

[5] https://alabama.port.training/

[6] https://houston.port.training/

[7] https://www.nmlea.org/academyonline-alex

[8] https://www.nmlea.org/post/transforming-the-classroom-into-a-digital-journey

security and environmental monitoring technologies. And in support of that mission, USF CMPS has stepped forward to offer participants in the MARSEC ADaPt program, an opportunity to expand the knowledge of its people – and give them credit for doing so. A degree program and a Continuing Technical Education program that will help to address many of the things that were outlined in the White Papers referenced earlier.

☐ **Assess, Consult, Train**

The NMLEA's **Approach to Comprehensive Training Solutions (ACTS**)[9] provides a pathway to improve and enhance the training programs currently in place at **A Port**, by assessing, evaluating, planning, designing and implementing effective programs, and utilizing the skills of Master Trainers, Facilitators, Coaches and Instructional Designers that are recognized nationally for their skills, knowledge and abilities. This is how we ACT (Assess, Consult, Train,) and it is how National Standards of Training are born. As part of the **MARSEC ADaPt** program, this service will be made available to **A Port**.

4.1 NMLEA, PortTraining, aLEX and USF Value Proposition

The following will be immediate, measurable and long-lasting benefits to **A Port,** when the Academic Advancement elements of the of the MARSEC ADaPt program are implemented.

- ✓ Immediate savings on required MTSA training with dramatically reduction in costs through the **PortTraining** learning portal.
- ✓ Access to a fully "**A Port's"** branded online learning management system – at no additional cost – that can provide a real time instant view of students learning process, (who has taken the training, how they did, when they took it, how long it took them, what they got right, where they took the training from, etc.) and the documentation necessary for regulatory compliance.
- ✓ Access to training that is available 24 hours a day, 7 days a week, 365 days a year to **A Port**'s employees, that will directly expand the reach and participation in your training programs.
- ✓ On-demand access to Master Trainers, instructional designers, and virtual/eLearning professionals who can assist in evaluating, assessing or transforming current instructor-led programs into virtual engagement successes that have a direct impact of the goals and objectives for **A Port**.
- ✓ NMLEA will act as an extension of **A Port's** Training Staff – without spending significant dollars on hiring new employees or contracting with outside entities.
- ✓ Direct access to USF CMPS, a Nationally recognized higher-education institution, and their degree/CTE programs designed specifically for the maritime industry and its unique workforce.

4.2 NMLEA Scope of Work and Deliverables

The NMLEA will lead the Academic Advance efforts, and will provide the following:

[9] https://www.nmlea.org/_files/ugd/7c4db2_fcc484f616074b808ef21f385a1aee79.pdf

a.) Conduct a Needs Assessment if requested/required, part of the Academy ACTs Program[10], to identify performance requirements and the knowledge, skills, and abilities needed by **A Port's** workforce to achieve specific requirements and objectives. An effective training Needs Assessment will help direct resources and effort to areas of greatest demand. The assessment shall; 1.) Address resources needed to fulfill the organizational mission; 2.) Improve productivity, and; 3.) Provide quality products and/or services as a result of implemented training. Note: A Needs Assessment is the process of identifying the "gap" between performance required and current performance, between actual performance and expected performance. When a difference exists, it explores the causes and reasons for the gap and methods for closing or eliminating the gap. A complete Needs Assessment also considers the consequences for ignoring the gaps.

b.) Provide an assessment of any current training, MTSA required and otherwise. (See ACTs Program[11]) to include a Training Audit - a systematic assessment of the efficiency and effectiveness of the design and delivery of a classroom training event. This step can be taken to evaluate existing training, through a review of the lesson plan(s) and the related participant materials, and an observation of classroom activities and outcomes. The audit will strive to answer the question: "Is there a high probability of learning through sound adult learning and trainer practices, principles and execution?" It will also answer another question relative to the organization: "Does it meet or exceed our mission and our strategic goals and objectives as an organization?"

c.) Provide access to **PortTraining** for all of **A Port's** employees at a 40% discount (e.g.: FSO course $695 - 40% discount = $417 **Port** price; Maritime Security Awareness course $50 – 40% discount = $30 price.)

d.) Design and produce "**A Port"** branded learning portal – at no additional cost.

e.) Provide the NMLEA's online Learning Management System and administrative privileges at no additional cost to **A Port** and provide administrative training to any selected port employees identified by leadership to manage the program.

f.) Provide help desk support to any students/learners who access the online learning portal.

g.) Allow on-demand access to Master Trainers, Instructional Designers and Educational leaders, to provide essential coaching, consultation and facilitation where needed as the workforce continues to evolve, improve and expand in its skills, knowledge and attitudes. Note that work required to develop additional courses will be quoted separately.

h.) Provide access to USF CMPS maritime specific courses and certificate programs, with preferred pricing as a participant in this program.

i.) Provide NMLEA's Exercise Designers, Planners, Evaluators to **A Port** as needed. Note: specific exercise engagements may require separate proposals and pricing, depending on scope.

[10] https://www.nmlea.org/_files/ugd/7c4db2_fcc484f616074b808ef21f385a1aee79.pdf

[11] ibid

5.0 INTERCONNECTIVITY, INTELLIGENCE AND INFORMATION SHARING

Understanding that our world is rapidly evolving, connectivity is key to our ultimate success, and security. Specifically in the areas of operations, threat intelligence, hazard response, and stakeholder involvement. When we look at who is the port connected with, how threat intelligence information is shared to and from federal, state and local entities, and how or who port operations are being shared with, the focus is not only on the security aspect of the port, but the resiliency as well. Is requires a look into information that diminishes the resiliency of **A Port**. Working with the National Maritime Intelligence and Integration Office (NMIO) and the University of South Florida Center for Maritime and Port Studies (USF CMPS), the NMLEA will lead the discovery process into a predicative and anticipatory variety of information sharing to include cyber, strategic competition, and environmental (weather, pollution, disease/pandemic, critical infrastructure conditions, etc.) data sets that can impact **A Port**, directly and indirectly.

5.1 Inter-Connectivity Value Proposition

- ✓ A better-connected port, makes for a "ready port" and for a more resilient port.
- ✓ Connecting to a premier National maritime intelligence office, provides **A Port** with access to information that can directly impact its safety and security.
- ✓ An ability to stay up to date with events, threats, and dynamic changes in the maritime environment, and maintain a readiness, preparedness and resiliency posture because of that connectivity.

5.2 NMLEA/NMIO Interconnectivity Scope of Work and Deliverables

a.) NMLEA/NMIO will examine current connections, information sharing practices, policies and procedures to point out potential enhancements that can improve **A Port's** readiness.

b.) NMLEA/NMIO will provide consultation, guidance and connections to intelligence sources, national level security initiatives, and maritime specific information that can directly impact **A Port**'s prevention, preparedness, response and resilience posture.

6.0 NAVIGATION

The last part of the DOMAIN is about navigating through the process of Maritime Security. We look at how the port enterprise responds to incidents and events. We look at what procedures, and processes are in place, and how the port fosters continuous improvement, and we look at their resilience. But one of the most important aspects of navigation is the "navigator." In this program, the NMLEA provides subject matter expertise in all the DOMAIN areas, to be that navigator for **A Port**.

The NMLEA will provide Administration of the MARSEC ADaPt program, conduct the Accreditation Assessment, and provide Consultation in all the areas discussed throughout this document.

6.1 NMLEA Navigational Value Proposition

- ✓ Direct access to subject matter experts that have directly impacted the Nation's maritime safety and security – at no additional cost.

6.2 NMLEA Navigation Scope of Work and Deliverables

a.) On-demand reach to maritime security SMEs for consultation, facilitation, coaching and leadership input as needed (up to 4 hours per month included in this package, at no additional cost.

b.) Administer, coordinate and collaborate with Accreditation Alliance partners in order to ensure timely, professional, and quality delivery of this program for **A Port** (up to 6 hours per month)

c.) Conduct the final Accreditation Assessment when all elements of the DOMAIN are in place, and **A Port** is ready for audit (approximately 40 hours)