

A SMARTER™ Approach to Maritime Security: Part Two

Port Digitization and MARSEC Accreditation

Standardized Security Solutions through the
Maritime Accreditation Alliance for **Research,**
Technology, Training, Exercises, Education,
Equipment and **Resources**



A White Paper based on a concept developed and produced by
The National Maritime Law Enforcement Academy
Written by: Mark R. DuPont, NMLEA Executive Director
January 2022

A SMARTER™ Approach to Maritime Security

- Part 2: Port Accreditation and Digitization -

Contents

Port Digitization and MARSEC Accreditation	1
Introduction and Overview.....	3
I. Maritime Security Situation Analysis: Where Are We Lacking “Smartness”?	5
A. Operational “Smartness”	7
B. Vulnerability Assessment “Smartness”	7
C. Training and Exercise “Smartness”	8
D. Cybersecurity “Smartness”	8
II. Laying out a “SMARTER” Course	10
Program Title	10
Program Goal.....	10
Program Mission.....	10
Program Objectives	10
Program Elements:	11
Program Benefits – and ROI:	14
Program Partners – A Maritime Security Alliance for Accreditation:.....	17
Program Advisors:	18
Program Implementation Strategies:	18
Program Projected Costs and Funding:	18
Program Milestones and Measures of Success:	19
III. In Conclusion: A Rising Tide will Raise All Ports.....	20



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -



Introduction and Overview

A Letter to Maritime Security Stakeholders

From Mark R. DuPont, NMLEA Executive Director and MARSEC ADaPt Program Manager

Dear Friends and Colleagues,

Back in March of 2017, we had released a White Paper titled *A SMARTER Approach to Maritime Security*¹, and in it we spoke about how we can look at the Maritime Transportation System (MTS) with all its parts, (the ports with all of the complexities and nuances, the public safety professionals protecting that domain and its 30 million workers², and the private sector trying to manage its functions and services) and explore how we can work together to solve some of the problems we face by providing “Security Solutions through the Maritime [Accreditation] Alliance for Research, Technology, Training, Exercises, Education, Equipment and Resources,” otherwise known as a “SMARTER” Approach.

This document will introduce you to an actual application of that SMARTER™ Approach to Maritime Security. It will show you how we can come together, and implement a program that will **Increase the Readiness and Resiliency** of our ports and maritime infrastructure through the creation of a National digital library, **Enhance our Security Capabilities** while dramatically **Reducing the Costs** of security regulatory compliance-related expenses (Vulnerability Assessments, Training, Exercises, and Cybersecurity Maturity,)

¹ <https://www.nmlea.org/research-and-white-papers>

² <https://www.ttnews.com/articles/ports-shipping-industry-responsible-26-us-gdp-study-says>



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

and **Implement a Nationally Recognized Baseline Standard** for those specific elements of maritime security – and **Accredit those ports that meet or exceed that standard**.

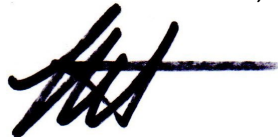
As stated in the original paper back in 2017, imagine the possibilities if maritime security in America was addressed cooperatively through an **Accreditation Alliance** in areas of Research, Technology, Training, Exercises, Education and Resources and through identified best practices in those areas. If federal agencies, private sector vendors, manufacturers, educational institutions, research organizations, exercise, training and consulting firms all came together to work under one umbrella, one banner, one name. And what if that one banner was based on an Accreditation process – so that a National Standard could be established, shared, and driven towards?

Through our diverse experience and the relationships we've fostered in this community over the last few decades, the picture we imagined has come into focus, and become a reality. Key strategic representatives and organizations have come forward to support and implement this initiative. They include (but are not limited to) ARES Security, HudsonCyber, Moran Shipping, the National Maritime Intelligence and Integration Office, the University of South Florida Center for Maritime and Port Studies, the International Propeller Club of the United States, and the American Association of Port Authorities.

The following pages will outline a SMARTER™ approach to our maritime security, developed by these key stakeholders. You are invited to explore and imagine the possibilities for you, your organization, and your country. At the end, there will be only one question: Are you on board? Are you part of the SMARTER™ community? Will you effect SMARTER™ Ports and Waterways?

I look forward to the journey, and the opportunity to explore this initiative with you, while making our ports and waterways SMARTER™.

Onward and forward, together.



"Logic will get you from A to B. Imagination will take you everywhere."

"To raise new questions, new possibilities, to regard old problems from a new angle, requires creative imagination and marks real advance...."

- Albert Einstein



I. Maritime Security Situation Analysis: Where Are We Lacking “Smartness”?

It is well known that the maritime transportation system (MTS) contributes to one-quarter of US GDP, or some \$5.4 trillion.³ And what has become abundantly clear through the pandemic, no global supply chain is independent of maritime transport. In fact, what the pandemic showed us (as well as a ship blocking the Suez Canal did) is that almost every supply chain is existentially dependent on the MTS – and disruptions can be catastrophic.

Seaports worldwide moved around 80 percent of global trade by volume and over 70 percent of global trade by value. And its importance is not slowing down, as global maritime trade continues to gather momentum; in 2018, the industry expanded by 4 percent globally—the fastest growth in five years.⁴ The pandemic will show those numbers growing even more.

Aside from critical infrastructure and supply chain importance, the maritime transportation system in the United States impacts a lot of workers. Between 2014 and 2018, the total number of jobs supported by cargo moving through America’s deep-draft ports increased to 30.8 million from 23.1 million⁵.

From a growing seaborne trade (including expansion of the Northern Route), growth in world fleet capacity, consolidation activity, and an increased pressure to track, measure and plan – the industry is thrust into managing, connecting, and implementing tools that streamline and improve the processes. Put simply, they need to “digitize” many of their functions. They need to become “Smart,” as illustrated in this [video by the Port of Rotterdam](#).



In a great paper published by Deloitte titled *Smart Port – Point of View*⁶, they lay the whole “Smart Port” issue out in simple terms. It’s worth the read. They point out that “Seaports are playing catch-up with the large transport & logistics players when it comes to developing

³ <https://www.ttnews.com/articles/ports-shipping-industry-responsible-26-us-gdp-study-says>

⁴ https://unctad.org/system/files/official-document/rmt2018_en.pdf

⁵ <https://maritime-executive.com/article/u-s-port-economic-impact-rises-dramatically>

⁶ <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/energy-resources/deloitte-nl-er-port-services-smart-ports.pdf>



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

insight driven solutions and IoT applications.” The paper goes on to say “Becoming a Smart Port means developing solutions to address the current and future challenges faced by seaports including spatial constraints, pressure on productivity, fiscal limitations, **safety and security risks** and sustainability. **Today’s technological and business model innovations can be a driving force behind the Smart Port.**”

But we are behind the curve. To quote the Deloitte paper again, “Even though some ports today are starting to come to terms with the importance and need for digitalization and IoT, **there is still a long road ahead to get to relatively mature Smart Port concepts.**”

So, what are we doing to get “smart” about how we protect this vital lifeline? Especially, as it relates to our security. In the Maritime Domain, there is a lot of evidence of our lack of “smartness,” as the world around us continues to advance in operational technologies, agility, adaptations, and security methodologies. This question becomes particularly important (and critical) when you look at the advances in all those areas by our adversaries – the people and states that want to disrupt, disarm, and debilitate our Nation through the lifeline that powers us. As domestic terrorism rises significantly (see Congressional testimony by FBI Director Christopher Wray ⁷), as foreign threats continue to mount (see quote by Director Wray), and as our digital world is expanding our attack surface exponentially, the criticality of our Maritime Security is becoming increasingly concerning.

“The greatest long-term threat to our nation’s information and intellectual property and to our economic vitality is the counterintelligence and economic espionage threat from China. It is a threat to our economic security and by extension, to our national security.”⁷

- FBI Director Christopher Wray

And it’s not just our adversaries – it’s climate, it’s accidents, it’s events that can (and will) impact our operations – and our lifeline. Just look at what the pandemic revealed to us, and the effects that such a disruption can inflict on the MTS. As stated in the *Cooperation on Maritime Cybersecurity* research paper published by the Atlantic Council, “The pandemic challenged the maritime industry with port closures, a new and shifting demand landscape, significant supply-chain disruptions, and operational questions around health and safety...The economic and security consequences of such a large-scale disruption shocked many—and proved how unprepared the MTS is for such systemic challenges.”⁸

So, where do we lack “Smartness” the most within the maritime world of operations? Where can we improve? Let’s look at these four specific areas.

⁷ <https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-091720>

⁸ <https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/>



A. Operational “Smartness”

The *Cooperation on Maritime Cybersecurity* research paper pointed out that things have grown exponentially in the maritime domain. “Much like many other critical infrastructure industries, operational efficiency and profit drive maritime transportation. That drive has caused a shift toward an even more complex environment—and complexity begets insecurity. As the size of the global economy and its reliance on maritime activity have accelerated, the maritime transportation sector has had to scale up its operations.”⁹



As we’ve scaled up operational capacities, and digitized much of our work functions – there is more that needs to be done, as outlined in the White Paper published by the World Bank Group titled, *ACCELERATING DIGITALIZATION, Critical Actions to Strengthen the Resilience of the Maritime Supply Chain*.¹⁰ The paper points out that “one of the key lessons learned early in the pandemic was the need to ensure business continuity of the critical supply lines, notably the maritime gateways, and the associated logistical chains.”

So, within those two paragraphs there are some critical words to pay attention to (they were underlined above): Operational efficiency and profit, an operationally complex environment, and as a result, complexity begets insecurity. Which leads to this question...

QUESTION: What if we could digitize our port – and our maritime security – providing continuity, resiliency, and saving significant amounts of money in the process?

B. Vulnerability Assessment “Smartness”

A requirement of the Maritime Transportation Security Act, Port Security Assessments provide the foundation for the effective implementation of maritime security measures at ports and port facilities. As Admiral Thad Allen stated during his tenure as the U.S. Coast Guard Commandant, “you’ve seen one port, you’ve seen one port.” Every one of our 300+ ports are different, with different types of risk and factors which affect an assessment. Which in turn suggests that Vulnerability Assessments can be both expensive and objective, based on who is doing them. The main key to port security risk assessment is choosing the right approach to provide the needed information without overworking the problem. Which leads to this question...



QUESTION: What if we could dramatically decrease the costs of vulnerability assessments, while providing an assessment tool that is active 24/7/365 (rather than once every five years) and through AI learns and improves every day?

⁹ <https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/>

¹⁰ https://unctad.org/system/files/non-official-document/tlb_20210304_report_wb.pdf



C. Training and Exercise “Smartness”

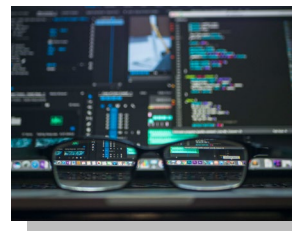
This is one area that we are extremely passionate about, for it is the foundation of everything we do, whatever our purpose, our industry, or our area of responsibility. For the training and preparation of people is as important as the air we breathe. Unfortunately, it’s also the area that falls prey to other operational or financial concerns. In a brief paper published in 2016 titled *Training Challenges: Adjusting to Incoming and Outgoing Tides*,¹¹ the NMLEA focused on training as it relates to change in our world of work, our area of responsibility and operation: the Nation’s waterways. We discussed how training in general has evolved, what some of the current challenges are in the maritime environment, and then gave some recommendations for our “fluid” workplace.

In another paper published by the NMLEA in 2017, *Navigating the Changing Seascape of Maritime Public Safety*,¹² we looked at the “4 P’s,”: People, Platforms, Processes and Performance. And in it, we talked specifically about the “Perfect Storm” affecting our People: increasing retirements and loss of institutional knowledge, retention issues, diversity shortfalls, and recruitment challenges. People are our most critical asset – yet it is one we struggle with to keep up in today’s workforce dynamics. Which leads to this question...

QUESTION: What if we could incorporate an “on demand” training system, that reached anyone, at any time, from anywhere? And what if we could dramatically reduce our training costs, while keeping up to date with an agile, adaptable, accessible, and affordable training program?

D. Cybersecurity “Smartness”

As stated in the *Cooperation on Maritime Cybersecurity* research paper referred to earlier, “The cyber-threat landscape in the MTS is similar to that of other critical infrastructure sectors. Global Positioning System (GPS) and Automatic Identification System (AIS) jamming and spoofing, attacks on less-than-secure OT and industrial control-system (ICS) devices, human targets, shipboard information and communications technology (ICT) systems – all are just some of the vectors that adversaries can and will use to attack the MTS. Ransomware, software supply-chain attacks, and social engineering are a few common tactics, techniques, and procedures (TTP) that have been used against the MTS. Potential targets and victims throughout the MTS include ships, ports, passenger and cargo shipping lines, shipbuilders and maritime manufacturers, and others. It is a complex and extraordinarily dynamic ecosystem that is difficult to defend. Cyberattacks represent an existential threat to the contemporary maritime industry, the smooth operation of which underpins modern society.”¹³



¹¹ <https://www.nmlea.org/research-and-white-papers>, *Training Challenges: Adjusting to the Incoming and Outgoing Tide*

¹² <https://www.nmlea.org/research-and-white-papers>, *Navigating the Changing Seascape of Maritime Public Safety*, pgs 4-8

¹³ <https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/>



A SMARTER™ Approach to Maritime Security

- Part 2: Port Accreditation and Digitization -

The paper goes on to say “all four of the world’s largest maritime shipping companies—A. P. Moller-Maersk (Maersk, as it is known, is part of the A. P. Moller Group), China Ocean Shipping Company (COSCO) Group, and Mediterranean Shipping Company (MSC)—have been hit by significant cyberattacks since 2017. Maersk, whose business operation systems were ravaged when the NotPetya malware spread from an infected Ukrainian tax-preparation software called MeDoc, spent more than \$300 million to return to full operations after ten days of repair and remediation. A reported 400-percent increase in maritime cyberattacks during 2020, along with a 900-percent increase in attacks targeting ships and port systems over the prior three years, point to a maritime industry in the crosshairs of malicious cyber actors. Despite this, the industry and its regulators have only slowly begun to move toward meaningful and systemic change.” That pretty much says it all. So, that leads to this question....

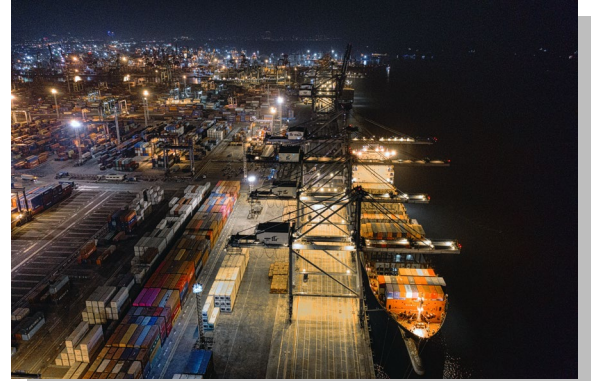
QUESTION: What if you could have access to a Cybersecurity Maturity Model, that through a visual “dashboard” could identify key areas that you needed to focus on, and provide “best practice” recommendations that would directly impact your resiliency – and lower your insurance costs?

With those areas explored, and the questions raised, the next section will answer them and plot a course towards a SMARTER Port. Read on.



II. Laying out a “SMARTER” Course

With the areas where we can get “SMARTER” identified in the previous section, and with the questions raised after each discussion – let’s lay out a pathway towards a solution. From discussions with a multitude of maritime stakeholders, and input from recognized subject matter experts, we have developed a solution package and plotted a course. Here are the program’s Goals and Objectives.



Program Title: Maritime Security Accreditation and Digitization Program (MARSEC ADaPt)

Program Goal: Take the Nation’s port security community into the digital age, by facilitating steps that can effortlessly, effectively, and efficiently enable that transformation, with clearly defined cost-savings and operational benefits, while establishing a National standard for Maritime Security.

Program Mission: Establish a Maritime Security Accreditation and Digitization Program (MARSEC ADaPt) for U.S. Ports, hosted by the National Maritime Law Enforcement Academy and powered by “best in class” security software, in partnership with the maritime domain’s leading organizations – and one that is recognized by the USCG, and establishes/demonstrates that accreditees have met a pre-requisite standard for Maritime Security Vulnerability Assessments, Training, Exercises and Cybersecurity Maturity.

Program Objectives:

1. Create a Digital Twin for every U.S. Port.
2. Provide the U.S. Coast Guard a national, digital library of maritime critical infrastructure.
3. Decrease the costs to ports for Vulnerability Assessments and provide continuous improvement through a 24/7/365 active “machine learning” tool – integrated with a port’s “Digital Twin.” Ensure that the tools are validated and recognized by agencies like DOD, DOE, and DHS.
4. Decrease the costs of training and exercises, through industry recognized software – integrated with a port’s “Digital Twin,” and allowing for accessible, affordable, adaptable, and accredited readiness and preparedness.
5. Provide a cybersecurity evaluation and measurement of maturity tool that is easy to implement, affordable, and allows port entities, their managers, and their leadership an easily and readily available “living” dashboard with quick access to improvement recommendations.
6. Provide access to regionally positioned port security specialists, and subject matter experts, so that “on the ground” knowledge, expertise, and experience can be provided quickly and easily.
7. Be able to demonstrate to participants in this program, first year return on investment, and long term, sustainable benefits.



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

Program Elements:

These are the parts of the Maritime Security Accreditation and Digitization Program, that make it an essential, foundational, and maturation step for every maritime stakeholder and port partner. What is underlined are the parts of the elements that are required in the execution of this Program.

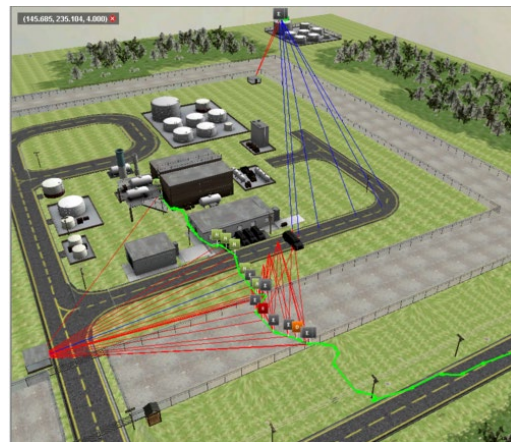
1. **A Digital Twin:** The first element of the program will provide organizations with a “digital twin” of their port and facilities. This will be a digital representation, or ‘twin’, of the physical components and systems, taking all the components of the physical entity – such as a port complex or terminal – and creating a 3D virtual map representation of the port, allowing interface and providing organized datasets for the user, that in turn can be used in the following components of the program.

The digital twin takes in data ranging anywhere from Internet of Things (IoT) types of sources, including AIS information and cargo-hold data, from carriers to performance statistics and status of port security elements, and functional parts of the operation.

Used as an operational tool, it can also be used as a vulnerability assessment tool, an exercise tool, and a training tool (see elements below), a Digital Twin will provide ports with a critical component that will directly impact preparedness, readiness, responsiveness and resiliency.

2. **Digital Twin Library:** The second element of this program is to create a digital library of all the Nation’s maritime critical infrastructure and provide access to the U.S. Coast Guard in order to better prepare for, respond to, manage the actions and mitigate the outcomes surrounding a significant port security event. This will be critical in our National Security, given the rising threats, both natural and man-made, and it will enable the Coast Guard to maximize the impact of the elements listed in the following paragraphs.
3. **Vulnerability Assessment Software:** Building off the Digital Twin component of the program, this element will provide ports with an intuitive user interface quickly create realistic 3D models of a facility that include interior and exterior features or structures, access points and entrances, natural features, and the placement of both active and passive barriers and detection tools. Once a site is modeled, the solution shall use Monte Carlo simulations in order to evaluate the comprehensive security design. An exclusive pathing algorithm will be utilized to determine the various pathways of adversaries, responders, and even natural hazards.

These assessments shall provide an organization with a complete understanding of their facility’s security and response to address vulnerabilities and optimize their configuration for both effectiveness and costs. The parameters must be easily changed within the model to address a wide range of security system configurations, threats and targets. Once the vulnerabilities and pathways have been identified and analyzed, users must be able to change and test new modeled sensors, systems, and procedures to improve their facility’s posture and



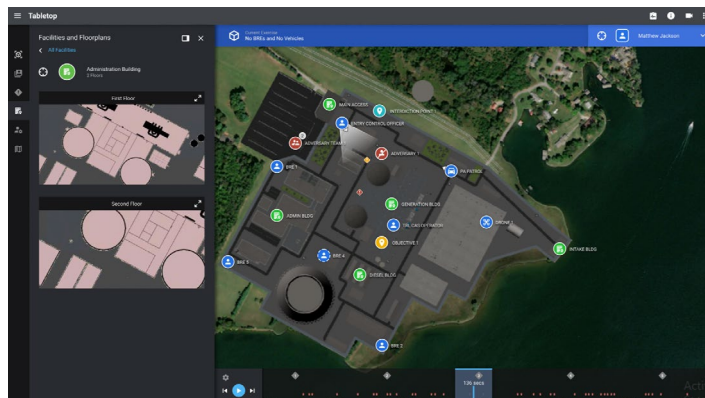
A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

thoroughly understand your return on investment. This quantitative approach shall provide a cost-effective means to continually assess risks and optimize a maritime partner's security effectiveness against their budget.

AVERT Security Design and Assessment Solutions was chosen to execute this element of the Program. Developed by ARES Security Corp, **AVERT** will provide unique modeling and simulation software that visualizes and quantifies the performance of security and response configurations. The results provide clients 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 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.¹⁴

4. **Virtual Exercise Software:** The Virtual Tabletop element of this Program will be able to mimic real-time scenarios and asset tracking for training purposes. Using the Virtual Tabletop, users must be able to run and control detailed simulations while commanding a virtual blue force against adversaries and see the real-time impacts of their decisions through a common operating picture. As a simulation runs, force commanders will be provided with limited information in which they must make decisions and position their forces based on adversary advances. The commander's decisions will update the agents and objectives within the simulation which in turn will change the simulations' outcome. Users must be able to select specific scenarios that are relevant to their facility and study the direct effects of each decision or an entire response.



Because of its DHS "SAFETY Act Certified" Software, the capability of **AVERT Virtual Tabletop** Physical Security software was chosen to run simulations on the various threats facing an organization. Upon discovering a facility's weaknesses and most likely attack avenues, executives will be able to host training exercises within those specific simulations. With the capability to simulate anything from terrorists and cyber-attacks to natural disasters, the Virtual Tabletop shall have a direct impact on a staff's preparedness, readiness, and responsiveness.

5. **Training Software & Learning Management System:** This element of the program will allow operators and their security forces to perform realistic training scenarios on a regular basis and stay

¹⁴ <https://aressecuritycorp.com/avert>



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

prepared for any situation, using the Digital Twin and tools/elements described in the preceding paragraphs. Additionally, any training for any personnel working in the maritime domain, will be integrated into online/virtual and instructor-led training tools, that can dramatically lower the cost of training, ease the scheduling of training, and allow all training to be readily and easily accessed.

PortTraining, operated by the NMLEA, began as the nation's only comprehensive seaport security curriculum with flexible delivery options and its online training management system was developed with Department of Homeland Security funding in 2005 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." Today, PortTraining is a resource for ports all across the country, providing an accessible, adaptable, and affordable means to meet the MTSA requirements – and much more.

aLEX is an NMLEA sponsored and developed product that provides a solution to an industry confronted with increased challenges to time, budgets, and an evolving workforce that public safety agencies are facing all across the country (see the White Paper: *Navigating the Changing Seascope of Maritime Public Safety*¹⁵). The Academy has used its knowledge, relationships, resources, adult learning expertise, and technology partnerships to provide a mobile, easily accessible, and affordable solution for every officer, department and maritime stakeholder. Put simply, **aLEX** provides a complete Learning Management System at no cost to its users and partners.

6. **Cybersecurity Maturity Model Software:** 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 program will provide a maturity-model methodology that will help an organization align with established best practices, nationally recognized standards, federal and international guidelines.

To successfully address the complexities of today's cyber threat environment, it is recognized that 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. And therefore, this element of the program must facilitate a shared obligation of all the 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

¹⁵ <https://www.nmlea.org/research-and-white-papers>

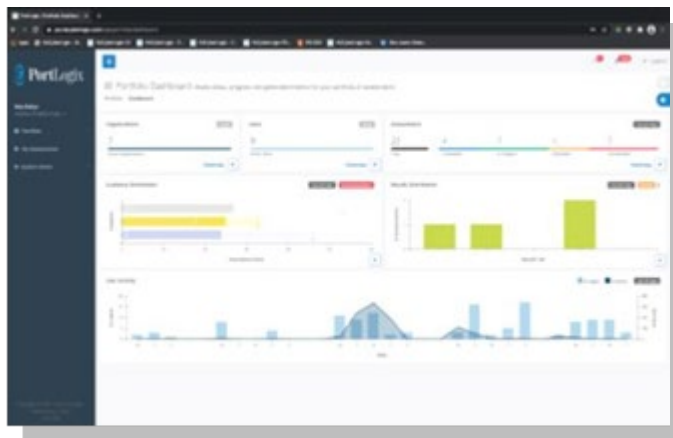


A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

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.

PortLogix is based on a maturity-model methodology that helps an organization align with the below standards, best practices, and guidelines:

- a. U.S. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (V1.1) (commonly referred to as the “NIST CSF”);
- b. NIST Special Publication 800-82 (Rev. 2) *Guide to Industrial Control Systems Security*;
- c. U.S. Department of Homeland Security *Cybersecurity Capability Maturity Model* (C2M2);
- d. Center for Internet Security *Critical Security Controls for Effective Cyber Defense* (V7);
- e. U.S. Coast Guard Navigation and Inspection Circular No. 01-20: *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Regulated Facilities* (2020);
- f. The IMO's *Guidelines on Maritime Cyber Risk Management* (MSC-FAL. 1/Circ. 3 (2017));
- g. ISO/IEC 27001:2013 RE: Information Security Management Systems – Requirements;
- h. European Union Agency for Cybersecurity (ENISA) *Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector* (December 2020); and,
- i. U.S. Customs and Border Protection Customs-Trade Partnership Against Terrorism (CTPAT) *Minimum Security Criteria: Cybersecurity*



7. **Deployed Port Security SME's Throughout the Country:** The last element, but just as important, is to provide ports with the availability and access to recognized security professionals to provide consultation, training, component facilitation, grant writing, and more. Because the dynamic post-pandemic workforce challenges are affecting every organization, port participants will have access to knowledgeable, experienced, and skilled trusted partners located throughout the country. Participants in this program will be able to reach out at any time, to people serving over 100 ports – and get what they need, when they need, from trusted partners.

Program Benefits – and ROI:

1. **Digital Twin:** A port is a point of significant economic activity, and the entry into our nation. Their impact on every aspect of our life and on every supply chain is tremendous.
 - a. A Digital Twin enables better management of assets with less environmental impact.



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

- b. With reliable and understandable data simulated in real-time, work becomes easier. Security becomes better, and vulnerabilities are identified.
 - c. Because ports are composed of many different activities and moving pieces, a Digital Twin can connect all these pieces and make them easy to see, control, manage and secure.
2. **Digital Twin Library:** Creating and providing a digital library of all the Nation's maritime critical infrastructure dramatically impacts the U.S. Coast Guard's ability to prepare for, respond to, manage the actions, and mitigate the outcomes surrounding a significant port security event. This is critical to our National Security, given the rising threats, both natural and man-made, and it will enable the Coast Guard to maximize the impact of the elements listed in the following paragraphs.
3. **Digitized and "Machine Learning" Vulnerability Assessments:** First and foremost, using this tool to conduct Vulnerability Assessments (required as part of the Maritime Transportation Security Act or MTSA¹⁶) will instantly, and dramatically impact the bottom line of a port or organization. Put simply, this software can conduct assessments every day, all day, and not be dependent on the opinions of individuals, but rather data driven facts as displayed through a tool that has been validated by DOD, DOE, and DHS. The money invested in this tool can be recaptured in one year, as illustrated for one organization when a \$23M planned capital expenditure was reduced to \$5M (\$17M savings) with improved effectiveness at a nuclear facility.
- a. **AVERT** assessments allows organizations to gauge the effectiveness of their overall security or response plans as well as the individual systems, staff & procedures.
 - b. Users can constantly validate the ROI of their entire security and response operations or run as-needed cost-benefit analyses for new acquisitions or projects to improve effectiveness while reducing cost.
 - c. **AVERT** solutions enable clients to model existing, new or temporary threats quickly to properly manage and respond to new scenarios.
 - d. **AVERT** users can assess their current security operations, improve their plans, and train on those new plans for how to address any type of security threat, such as Active Shooters, Natural Disasters, IED's and Drones, at any type of facility.
 - e. This process removes the potential for human error, or reliance on analysts, and allows organizations to generate any number of customized reports that can accurately display aggregate results from thousands of simulations with complete accuracy.
 - f. These government-validated reports provided from the assessments allow teams to determine the effectiveness of their overall security or response plans and show in detail how a change will increase effectiveness and at what cost.
4. **Virtual Exercises:** Physical tabletop exercises (also required as part of the MTSA) are both time consuming and expensive; furthermore, the drills leave the results of decisions up to chance or a roll of the dice. Using the Virtual Tabletop software allows participants to see the most likely effects

¹⁶ <http://www.chemicalsecurity.com/Assets/maritimetransportationsecurityactof2002.pdf>



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

of their decisions. After each decision is made, the scenario is re-simulated and updated so participants can see how their decisions affect the simulation's outcome. By removing the limitations and guesswork involved in regular tabletop drills, this virtual training environment goes well beyond the capabilities of normal exercises – while saving money in the process

5. **On-Demand Training:** As we attempt to compensate for changes, adjustments, operational challenges, budget constraints and time shortages in a post-virus landscape, one thing is becoming increasingly clear: learning needs to be more flexible, accessible, available, and affordable to people at the precise moment it is needed. Digital tools can provide this flexibility, making the task of continuous learning easier and more effective than ever. This program provides easily accessed training at any time, from anywhere, by anyone. Training can now reach people quickly, and not be dependent on trainer or worker availability. Most importantly, the tools and SMEs being utilized here are recognized around the country for their experience, knowledge, and extensive results for work with DHS, the USCG, ports, agencies, and stakeholders across the maritime domain.
6. **Cybersecurity Maturity:**
 - a. Save money by focusing resources (people, technology, budgets) on the organization's highest priority needs.
 - b. Brief boards and investors with **PortLogix'** intuitive scorecard metrics;
 - c. Inform planning and budgeting activities across twelve operational areas;
 - d. Benchmark internal growth and compare progress against industry peers;
 - e. Develop internal knowledge, skills, and competencies by investing in staff rather than expensive cybersecurity consultants; and,
 - f. Empower and educate staff through hands-on analysis;
 - g. Launch an award-winning cybersecurity program in as little as one or two days;
 - h. Drive internal collaboration by organizing assessment teams with stakeholders from across the organization;
 - i. Foster a cyber-aware culture through consensus-based analysis and assessment;
 - j. Streamline and standardize internal audit and inspection activities; and,
 - k. Initiate assessments and teams in minutes;
7. **National Network of Industry Recognized Port Security SME's:** Lastly, but just as important, is the availability and access to recognized ports security professionals. Not every port has the staff and experience necessary to facilitate these components, deliver training, access grants, or provide "on the ground" knowledge and perspective. Participants in this program will be able to reach out at any time, to people serving over 100 ports – and get what they need, when they need, from trusted partners. This dramatically impacts your personnel costs, for the services are on-demand, rather than having to hire full-time employees.



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

Program Partners – A Maritime Security Alliance for Accreditation:

The following assembly of partners in this endeavor were chosen because they are each already recognized in their respective areas as “Best in Class, or as “Best Practices”.

1. **The National Maritime Law Enforcement Academy (NMLEA)**: Following a vision and the leadership of Admiral Siler, a former U.S. Coast Guard Commandant, the National Maritime Law Enforcement Academy (NMLEA) was established in 2000 to fill a capabilities gap that continues to effect law enforcement, emergency response, port security and defense operations on the water across America and internationally. The NMLEA provides education and training for professionals who patrol, protect and preserve our maritime domain. As an extension of an agency's training staff, the NMLEA provides nationally recognized training and exercise programs, assisting agencies and departments of all sizes to improve tactical and response operations within an agency, with coordination among partners at times of catastrophic events exercising the National Incident Management System (NIMS).
2. **ARES Security Corporation**: Since 1999 when the company began developing the AVERT risk assessment solution as ARES Corporation with the support of the US Department of Defense, the mission has been to provide solutions that safeguard a diverse client base’s critical assets from the World’s dynamic threat environment. On October 1, 2012, ARES Security Corporation was officially established as a stand-alone company to invest in future technologies and continue delivering the AVERT solutions to a growing list of government and commercial clients. With extensive expertise in developing advanced solutions, ARES has delivered multiple complex solutions in various regions, states, and countries. The AVERT family of products are currently being utilized in 67% of the North American nuclear reactors, U.S Air Force Bases, public safety departments, education, transit agencies, and a third of the top-tier seaports.
3. **HudsonCyber**: Combining decades of knowledge and expertise with best-in-class capabilities and technologies, HudsonCyber designs and delivers practical and sustainable cyber security and cyber risk management solutions to clients around the world, supporting the global maritime transportation industry, spanning ports, terminal operators, commercial shipping, oil/gas companies (both national and commercial), flag states, insurance companies, and national and regional government bodies.
4. **Moran Shipping - Office of Maritime & Port Security (MOMPS)**: For over 75 Years MOMPS has provided services, technology, equipment, manpower and consulting to the maritime industry - representing niche organizations, governmental agencies, ship owners, operators, charterers, cargo facilities, seafarers, ferry operators, and virtually all sectors within the maritime realm in the US and globally. MOMPS provides a real time, boots on the ground perspective unmatched by any other in the security realm. With 20 locations directly servicing over 100 U.S. ports with remote offices and staff, the MOMPS team can work globally on assignments and projects anywhere in the world. MOMPS is the only organization dedicated exclusively to maritime and capable of providing security in all 361 U.S. ports and around the world.



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

5. [The University of South Florida, Center for Maritime and Port Studies \(CMPS\)](#): The mission of the CMPS is to address the needs of the coastal community stakeholders: (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 security and environmental monitoring technologies. These capabilities will be developed from CMPS's extensive experience in these areas, including a 20-year-plus collaboration with the local port and maritime transportation community, its work with the National Oceanic and Atmospheric Administration (NOAA) Office of Coastal Management (OCM) on their *Port Tomorrow Resilience Planning Tool*, and its 15-year experience leading the *Alliance for Coastal Technologies*.

Program Advisors:

1. The National Maritime Intelligence and Integration Office
2. Oak Ridge National Laboratory
3. United States Coast Guard and United States Navy Flag Panel
4. Port Tampa Bay
5. American Association of Port Authorities
6. The International Propeller Club of the United States



Program Implementation Strategies:

1. Seek U.S. Coast Guard support and recognition of the Program
2. Demonstrate the Proof of Concept with four key ports identified in Pilot Program
3. Present Program Overview to all Area Maritime Security Committees
4. Provide webinars for Program educational purposes
5. Educate the industry, through identified conference speaking engagements, provide the overview and seek additional partnerships/contributors
6. Pursue Port Security Grant funding recognition
7. Identify other grant program opportunities

Program Projected Costs and Funding:

The costs to implement this program will be standardized for every port in the country. For less than the cost associated with one exercise (costs reported in national studies can be as much as \$80k for a Tabletop¹⁷, with Functional and Full-Scale exercises being exponentially more) or less than the costs of a Vulnerability Assessment, a port can “ADaPT” and become “digitized”, while being recognized through

¹⁷ <https://www.ciodive.com/news/tabletop-exercises-security-breach-immersive-labs-osterman/583607/>



A SMARTER™ Approach to Maritime Security - Part 2: Port Accreditation and Digitization -

Accreditation for its accomplishment. The cost for a port to “adapt” with all these elements will be **less than \$75,000 per year, or on a monthly basis, less than \$6500 per month** as a Software as a Service (SaaS).

Funding for this program, if not from normal operational funds, can come from, Port Security Grants (\$100 million each year since 2016), Infrastructure Grants (FY2022 the Infrastructure and Jobs Act/Bipartisan Infrastructure Law, appropriated \$450 million to the Port Infrastructure Development Program) and others.

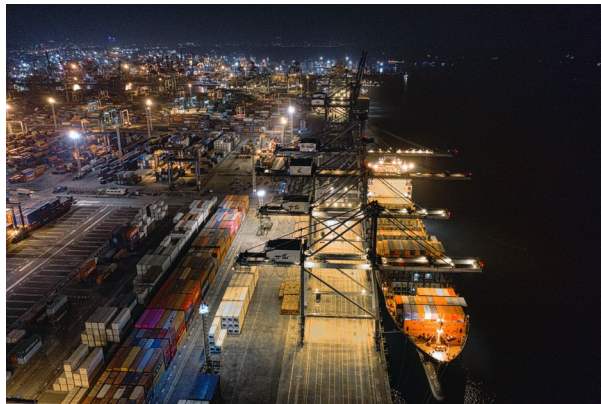
On a national level, funding for this program can come from Coast Guard funding/appropriations, and from the Department of Defense funds as it relates to the Nation’s strategic ports.

Program Milestones and Measures of Success:

The team who worked on the development of this program project the following milestones: 25 Ports MARSEC Accredited in Year 1, 50 ports in Year 2, 100 ports in Year 3, 300 by Year 5.

Additionally, the following Measures of Success will provide evidence of the program’s validity, usefulness, and national adoption:

- ☑ Individual ROI for each port in first year of Application – evidenced by measurable, reportable, and sustainable reduction in personnel, exercise, training, and vulnerability assessment costs.
- ☑ An MOU/Endorsement from key stakeholder organizations, government agencies, private sector contributors.
- ☑ A measurable increase in number of port workers reached and their subsequent use of on-demand training resources – directly impacting our nation’s port readiness.
- ☑ A dramatic increase annually in the number of ports in America who have adopted a cybersecurity maturity model framework that fosters “whole of community” collaboration and promotes/facilitates continuous improvement – directly enhancing our maritime resilience.
- ☑ The implementation of a Digital Library, and its use by the U.S. Coast Guard in planning, exercise, and response coordination – directly impacting our maritime preparedness on a national scale.



III. In Conclusion: A Rising Tide will Raise All Ports



To repeat some of the comments made in the original White Paper titled *A SMARTER Approach to Maritime Security*, we hope this dissertation has generated thoughts in your mind about how we can approach our security efforts a little differently, yet with profound benefit to our collective maritime community. We can do things better together, than we can individually. When we put our resources, minds and skills together and are focused on one objective, the results are amazing. We call it the “Apollo 13 Effect.”

When we think about this particular SMARTER application of that “whole of community” thought process, there is an immediate and lasting impact on our ports as individual entities, and on our maritime domain in its entirety. Through this Program, ports can get more secure, can train more people, can make better decisions, can be more resilient, and have access to people with the knowledge, skills and attitudes necessary to enhance their operations. All of that for less than what they are paying for those things now.

If we establish, implement and facilitate this Maritime Security Accreditation and Digitization Program – America will be better, stronger, advanced and secure through a National Standard of performance. If you perform better, you compete better, you operate better. And if we raise the tide in one port – we raise the tide for all ports.

Time to plot our course - onward and forward.

