

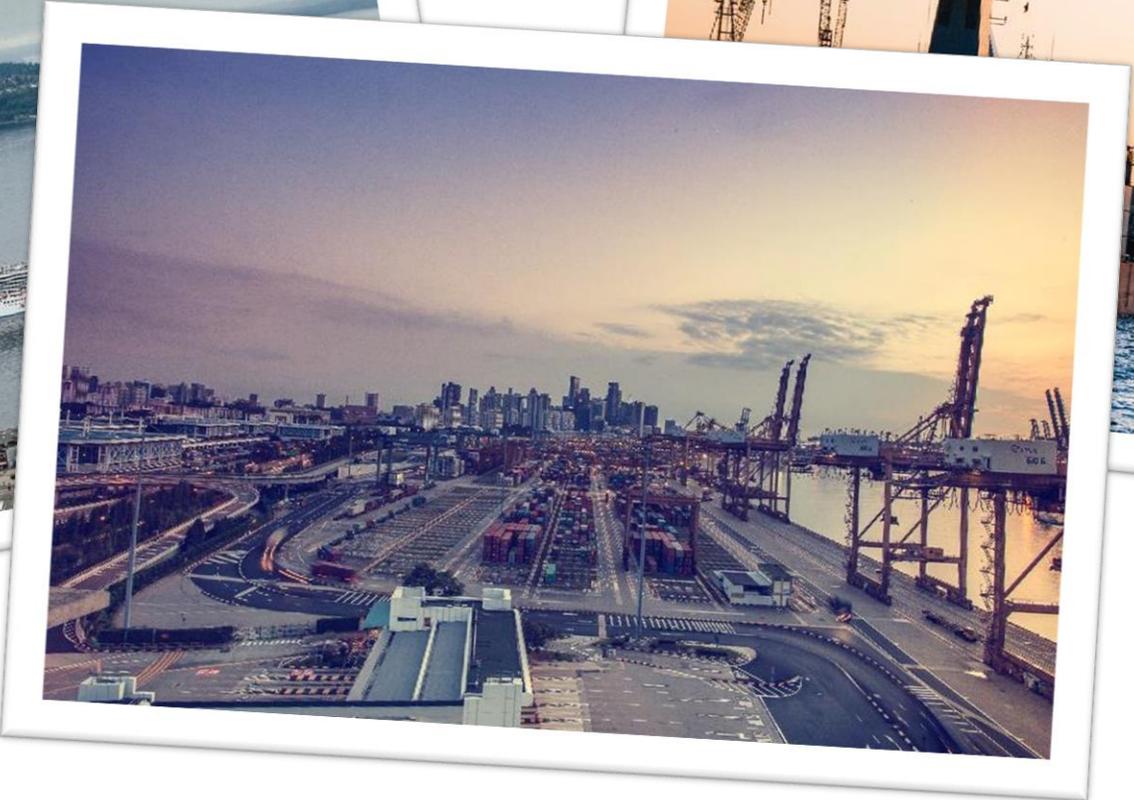
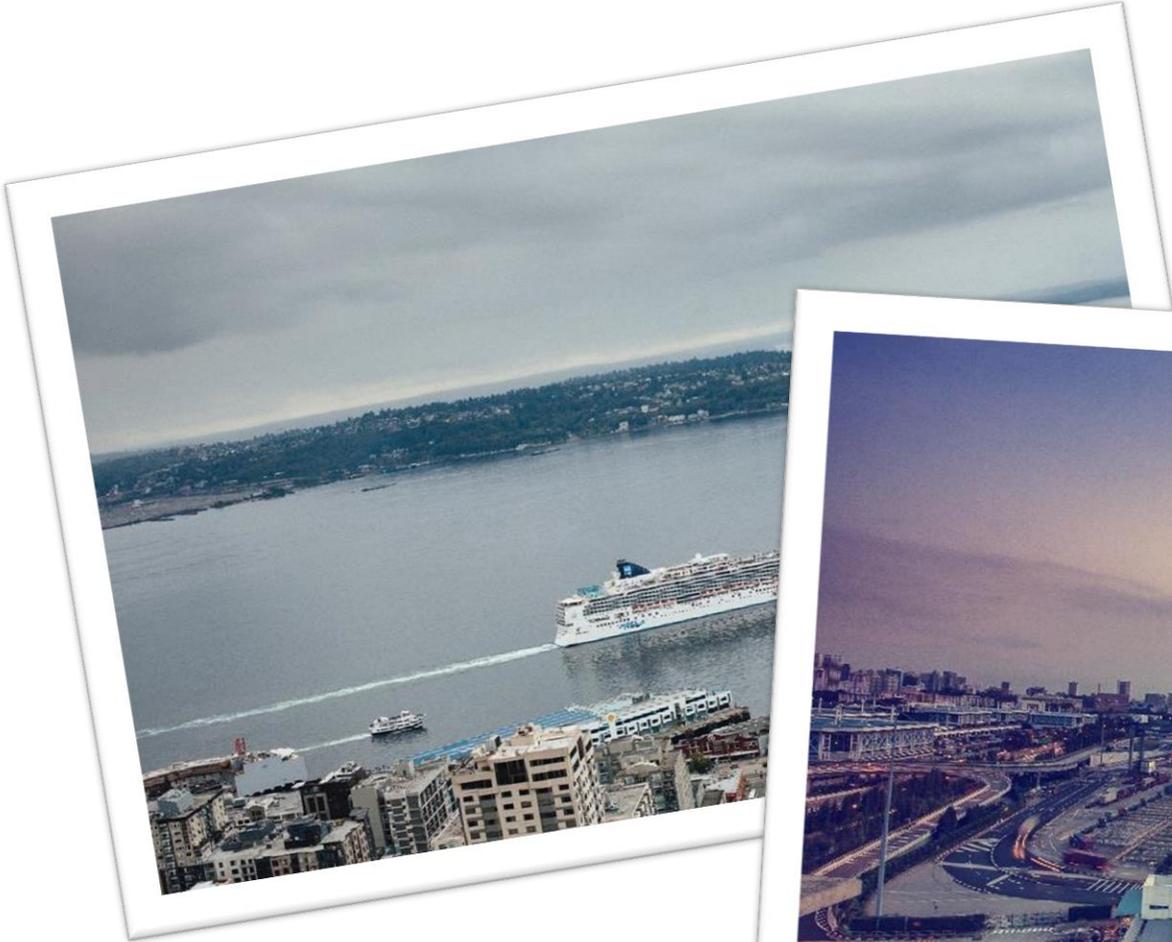


*An overview of “MARSEC ADaPt,”  
and how it can impact the Nation’s  
maritime DOMAIN.*



**Making SMARTER Ports while  
saving money, time and effort**

To begin, let's take a picture...



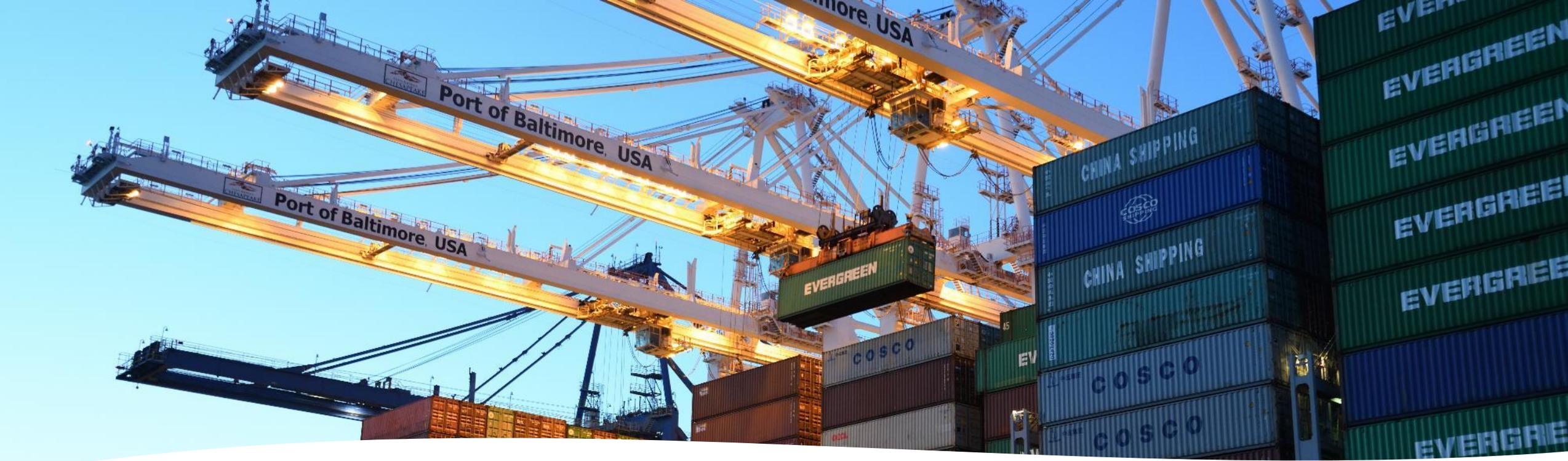


## Current Snapshot...

**“Seaports are playing catch-up** with the large transport & logistics players when it comes to developing insight driven solutions and IoT applications.”

“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.**”

*Deloitte Smart Port – Point of View*



## Current Snapshot...

**“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.**”

*Cooperation on Maritime Cybersecurity* Research Paper  
Published by the Atlantic Council



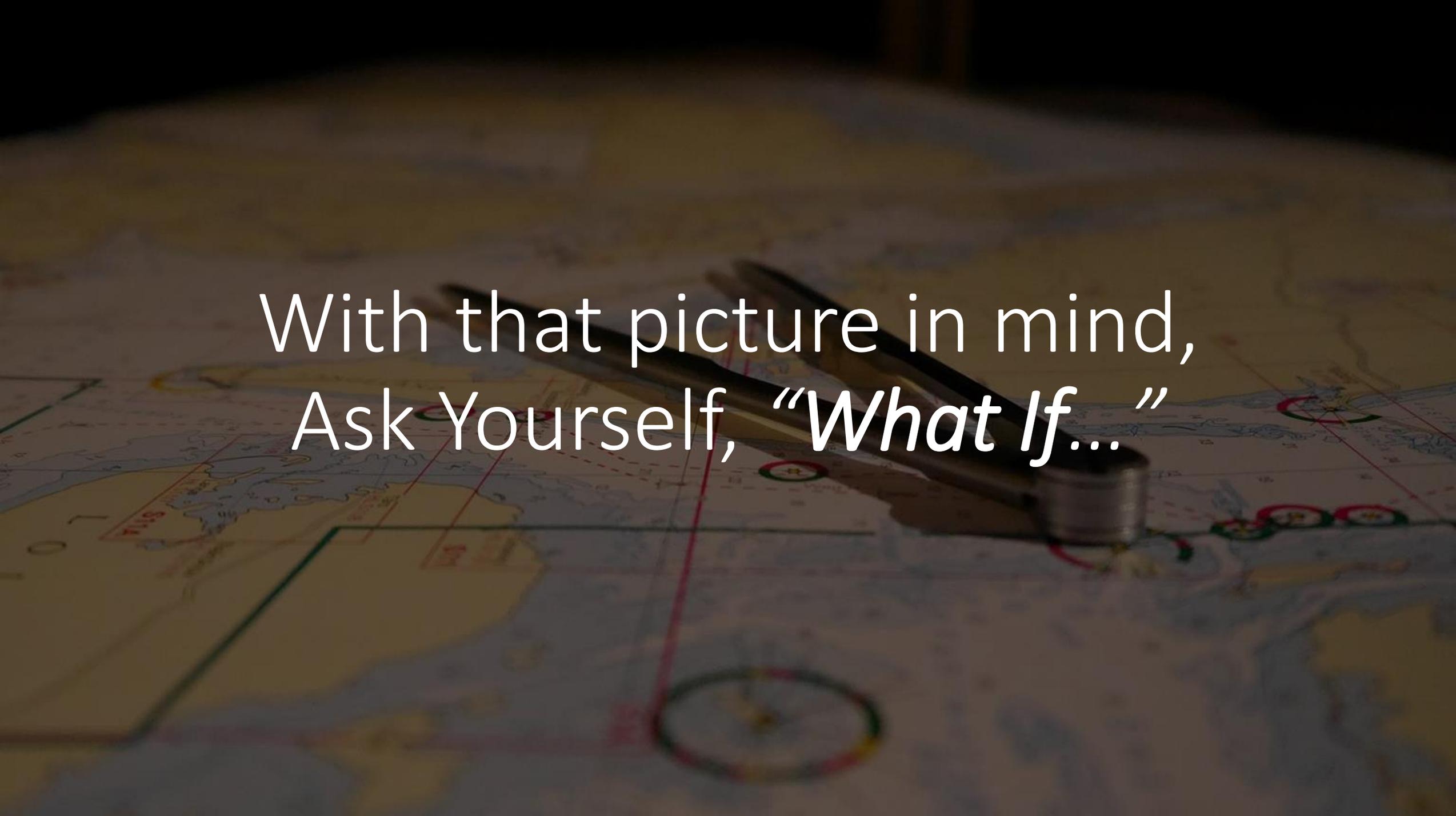
## Current Snapshot...

“Much like many other critical infrastructure industries, **operational efficiency and profit drive maritime transportation.**”

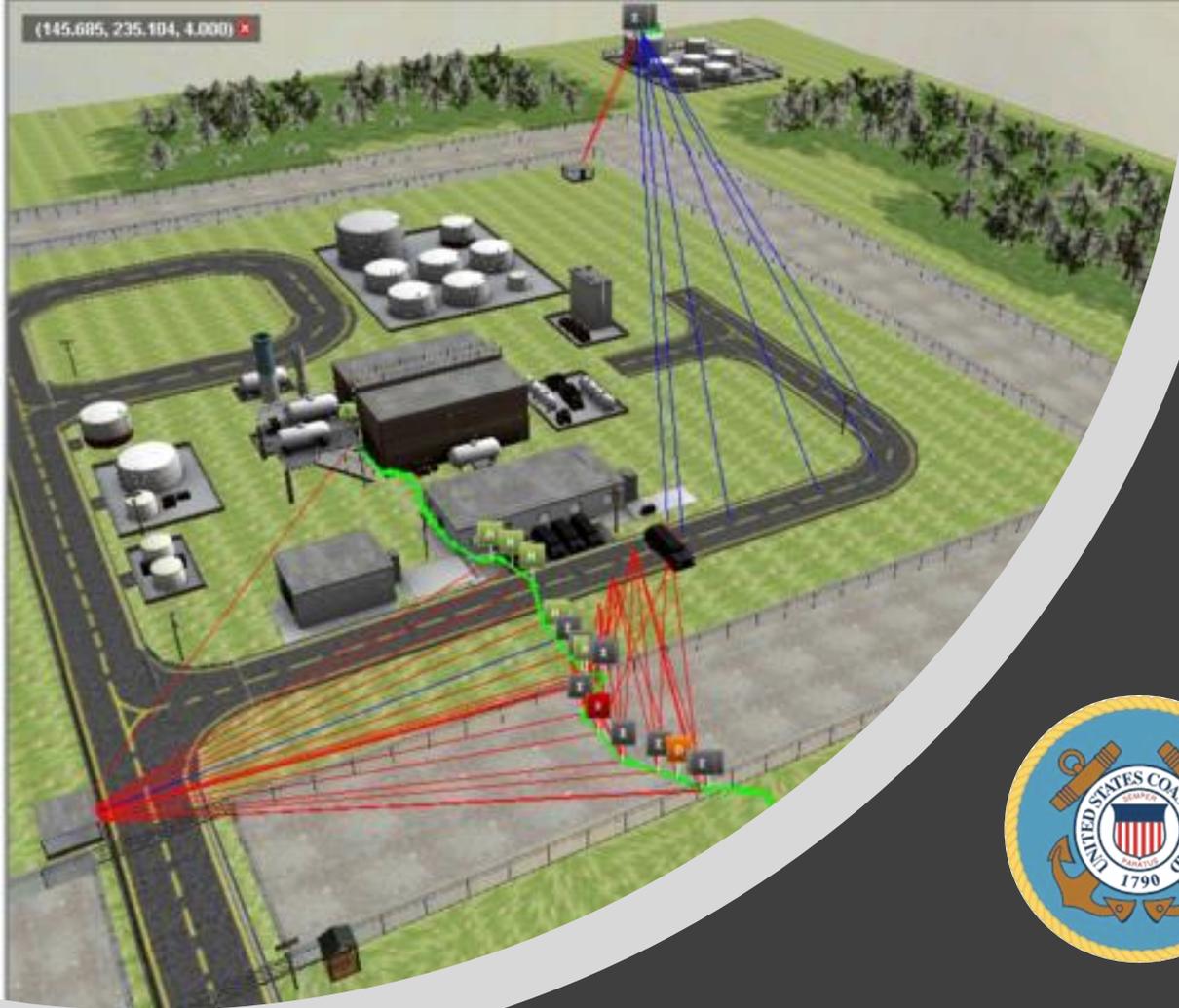
“That drive has caused a shift toward an even more complex environment—and **complexity begets insecurity.**”

“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.**”

*Cooperation on Maritime Cybersecurity* Research Paper  
Published by the Atlantic Council

A pair of metal compasses is shown in the foreground, resting on a map. The map features various colored lines and circles, suggesting a technical or surveying drawing. The text is overlaid in white, centered on the image.

With that picture in mind,  
Ask Yourself, "*What If...*"



*What if...* we could **digitize your port** – and your maritime security – providing continuity, resiliency, and saving significant amounts of money in the process?



*What if...* we could digitize **all of the Nation's ports**, and create a Digital Library for the U.S. Coast Guard?

*What if...* we could dramatically decrease the costs of vulnerability assessments, exercises and training?

*What if...* we could provide an assessment tool that is **active 24/7/365** (rather than once every few years)?

*What if...* you had a security assessment tool that through AI/Machine Learning, **learns and improves every day**?

*What if...* the tools you used for all of this were **validated and recognized** by the DoD, DoE, and DHS to protect America's critical infrastructure?



#### DoD Accredited

- Sponsored by the Defense Threat Reduction Agency, US Air Force & US Navy
- Accredited for assessment at nuclear storage facilities



#### DoE Accredited

- Depended on to evaluate vulnerabilities at NNSA facilities
- Used to optimize force protection capabilities at high-consequence facilities



#### DHS Certified

- The only SAFETY Act Certified Software to conduct vulnerability assessments
- Provides users liability indemnification from acts of terrorism



#### World Institute of Nuclear Security Published

- Projects featured in the Best Practices Guide for Nuclear Security
- WINS ([www.wins.org](http://www.wins.org)) is a nuclear security best practice organization



*What if...* you could have access to and implement a **Cybersecurity Maturity Model**, that is recognized by Lloyd's as Digital Innovation Winner?

*What if...* through a visual “dashboard” you could identify key areas that you needed to focus on?

*What if...* you were provided “best practice” recommendations that would directly impact your resiliency – and lower your insurance costs?

*What if...* we could incorporate an **“on demand” training system**, that can be reached by anyone, at any time, from anywhere?

And *what if...* we could **dramatically reduce your training costs**, while keeping up to date with an agile, adaptable, accessible, and affordable training program?





*What if...* we were able to provide access to local/on the ground **Port Security Subject Matter experts**, located throughout the country?

*What if...* we were able to **share** and give every port the **knowledge, skill, experience, and abilities** necessary to implement and enhance their Maritime Security capabilities and resilience?



And *what if*... the ports that did all of these things were **recognized – Nationally**, by their peers, their customers, the U. S. Coast Guard, and by their insurers?





# A R E S

S E C U R I T Y



## What if, you Collaborated with Public/Private Stakeholders...

- ☑ Security software recognized and validated by DoD, DoE (protecting over 65% of the Nation's nuclear facilities) and is DHS "Safety Act Certified."
- ☑ Cybersecurity maturity model software that facilitates "whole of community" buy-in, and heralded by Lloyd's as a Digital Innovation Winner.
- ☑ A shipping company with Port Security SMEs that has been a trusted resource for over 75 years.
- ☑ An online learning portal, developed for the USCG back in 2010, that provides affordable, accessible, and adaptable MTSA type training for ports across the country.
- ☑ A Navy organization tasked by the Director of National Intelligence to ensure that intelligence and information that matters to the Global Maritime Community of Interest is getting to those who need it.
- ☑ A technology company, owned by LSU, collecting and analyzing cybersecurity data from ports around the country – in service to the Navy Research Lab and USCG
- ☑ A University recognized for its professional development of the maritime transportation industry; and continuous research on security, sustainability, and resilience of the maritime transportation system

The answer to your  
questions...

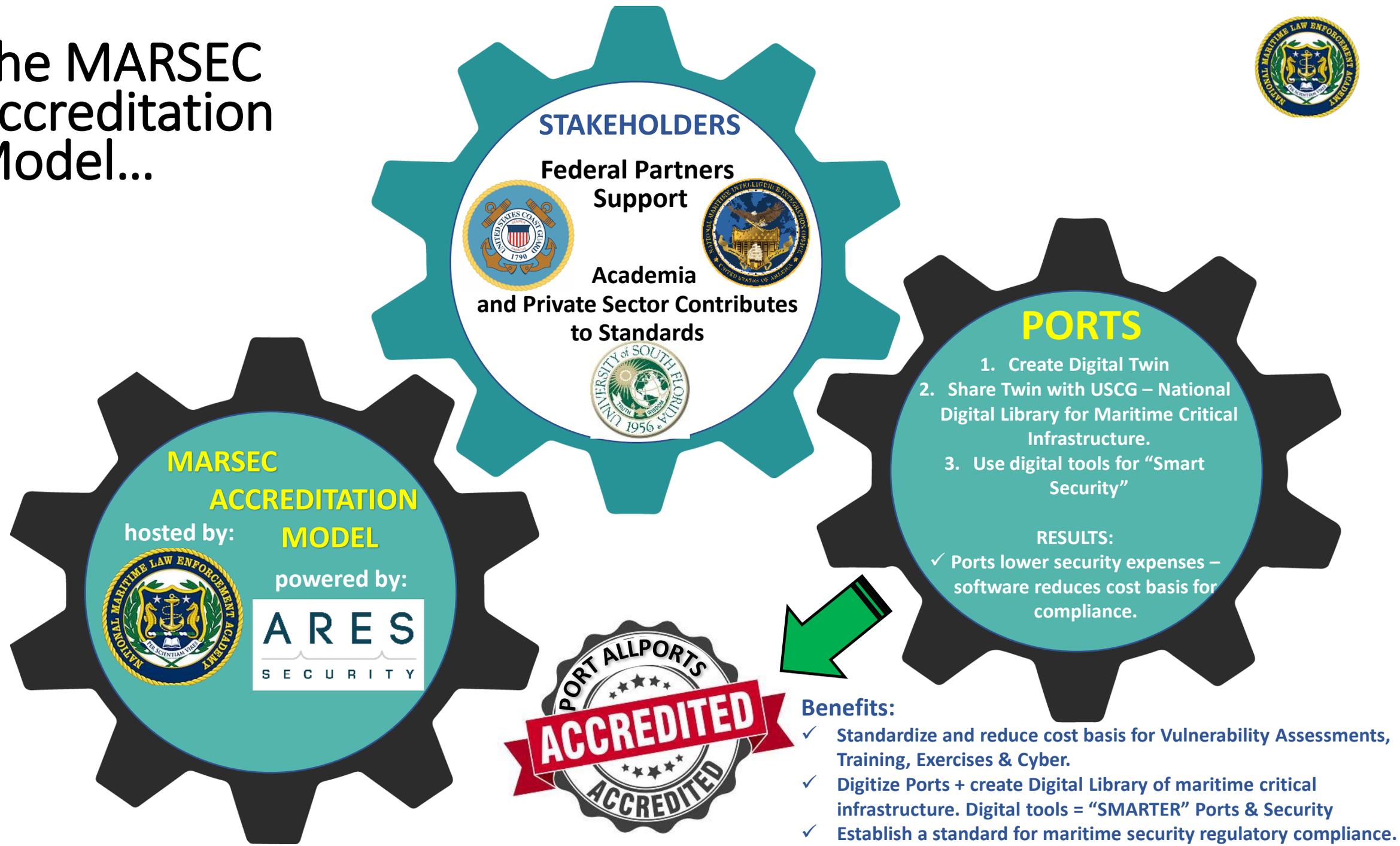
The Maritime Security  
Accreditation and  
Digitization Program

**MARSEC “ADaPt”**



**Become MARSEC  
“ADaPt” Accredited**

# The MARSEC Accreditation Model...



# How Does a Port get MARSEC Accreditation?



## Three Primary Requirements

### Create Digital Twin

*A digital twin is a virtual representation that serves as the real-time digital counterpart of a physical object or process.*



### Share Twin with USCG

*Collaborate to achieve National Security objectives and a Common Operational Picture in the Maritime Domain.*



### Establish & Validate Security Standards

*Vulnerability Assessments, Training, Exercises & Cyber processes analyzed and validated by NMLEA*



### Benefits

Annual Recurring Savings on Vulnerability Assessments, Training, and Exercises

### Benefits

Enhanced Maritime Security Readiness and Support for National Security Objectives

### Benefits

Standards-based approach to common maritime security tasks. Regulatory compliance support.



# Nationally Recognized Software Support as the Foundation...

*The National Maritime Law Enforcement Academy has selected ARES AVERT and HudsonCyber PortLogix software to support the MARSEC Accreditation Initiative. This software has been purpose built to optimize Vulnerability Assessment, Training, Exercise, and Cyber requirements in support of maritime critical infrastructure protection.*



ARES will work with maritime critical infrastructure owners/operators to create a digital twin for each site that requires protection. The Twin will be stored in an encrypted library and available to support Assessments, Training, Exercises and Cyber security.



## Vulnerability Assessments

ARES will use the AVERT PS software to perform maritime Vulnerability Assessments in support of the Facility Security Assessment mandated by the Maritime Transportation Security Act.



## Training

ARES AVERT, combined with a Port's Digital Twin, represents a powerful training tool that can deliver cost effective, remote training tied directly to the digital assets. Additionally, the NMLEA's aLEX and PortTraining tools will impact training



## Exercises

By using the Digital Twin, ARES can use AVERT Virtual Tabletop to create an immersive environment that is more interactive, realistic, and measurable than existing virtual exercise tools.



## Cyber

Hudson Cyber's PortLogix SaaS tool is based on a maturity model methodology that supports compliance with IMO, NIST, and USCG/MTSA cyber security guidelines.

# Leading to recognition as a MARSEC “ADaPt-ed” DOMAIN

## ***DIGITIZATION:***

Does the port have a Digital Twin, a virtual representation of the physical site and facilities that are being protected?

Has that Digital Twin been shared with the USCG?

How is the Digital Twin being used?

## ***OPTIMIZATION:***

Leveraging that digitization, does the port have a means of conducting continuous vulnerability assessments (vs. done just once every five years)?

Do they use machine learning technologies recognized by the Department of Defense, Department of Energy, and the Department of Homeland Security?

## ***MATURITY:***

Does the port have a means of looking at its cybersecurity posture, and assessing its maturity in the areas of risk management through a multi-discipline, consistent engagement, (vs. an annual checklist-based approach) that aligns with established best practices, nationally recognized standards, and federal/international guidelines for cybersecurity?

Does their cybersecurity risk assessment stimulate in-person (or virtual) cross-functional collaboration, promote awareness, and enhance communication and information sharing?

Does their process facilitate capability growth and cybersecurity resilience over time?

## ***ACADEMIC ADVANCEMENT:***

How is the port advancing its workforce? What training tools are in place and utilized to not only ensure regulatory compliance, but to also expand the knowledge, skills, and attitudes of its employees?

How are records of training kept (Learning Management System)?

Is the training accessible, affordable, adaptable in this new mobile environment?

Are continuing education opportunities available and promoted?

Is the training program linked to a national institution?

## ***INTER- CONNECTIVITY, INTELLIGENCE, AND INFORMATION SHARING:***

Who is the port connected with?

Is threat intelligence information being shared to and from federal, state, and local entities?

Is any information that diminishes the resiliency of port operations being shared, and with whom?

Is there a predicative and anticipatory variety of information sharing to include cyber, strategic competition, environmental and other critical data sets that can directly impact a port's safety and security?

## ***NAVIGATION:***

The last part of the DOMAIN, how does the port enterprise respond to incidents, events?

What are the procedures, and processes?

How well do they do it, as evidenced in actual events or in exercises?

More importantly, how do they ensure continuous improvement?

How resilient are they?





**\$75,000/Yr**  
*Or as low as*  
**\$5,000/Month**

## *With Benefits...*

- For the Port:
  - ✓ ROI in first year
  - ✓ 24/7/365 Vulnerability Assessments, Exercises and Training
  - ✓ “Machine Learning”
  - ✓ Peer-to-peer relationship learning
  - ✓ Online, On-Demand LMS
  - ✓ A more “whole of community” approach to cybersecurity
  - ✓ An enhanced security readiness, response and resilience
  - ✓ Affordable, adaptable, accessible
- For the Nation (USCG):
  - ✓ A National Digital Library
  - ✓ A National level exercise, planning and response tool
  - ✓ National level data collection and analysis
  - ✓ A National rise in Cybersecurity Maturity

The cost and benefit to “ADaPt,” and become a SMARTER Port?



**Become MARSEC  
"ADaPt" Accredited**

# The Maritime Security Accreditation and Digitization Program

Mark R. DuPont, Executive Director  
National Maritime Law Enforcement Academy

(d) 305-240-0934

(e) Mark.DuPont@nmlea.org

(w) www.nmlea.org

[www.nmlea.org/marsec-accreditation](http://www.nmlea.org/marsec-accreditation)