PORT SECUTITY GRANT PROJECT:

Maritime Security Accreditation & Digitalization Program

DIGITIZE PORT SECURITY AND REDUCE COSTS. AUTOMATE ASSESSMENTS, TRAINING & EXERCISES.

Apply Grant Funding to Become a "Smart Port"

The National Maritime Law Enforcement Academy's MARSEC Accreditation Program provides ports and facilities with an opportunity to have a third party verify and validate their baseline maritime security posture. NMLEA Accreditation emphasizes cybersecurity preparedness, and encourages digitalization and the use of digital tools to optimize security compliance tasks. And the MARSEC Accreditation Program is grant eligible. Benefits of NMLEA Accreditation:

- Validate maritime security proficiency and readiness
- Apply a Digital Twin (3D model) to reduce security compliance cost and time – automate security assessments, training, and exercises
- DHS SAFETY ACT Certified technology lowers risk and improves insurability
- Easily train and share information with external stakeholders

PORT SECURITY GRANT PROGRAM ELIGIBLE

ARES

HudsonCyber
Managing Cyber Risk

www.nmlea.org/marsec-accreditation

MARSEC Accreditation & Port Security Grant Program

GRANT ELIGIBILITY

1 CYBERSECURITY

Ports and facilities will have a means of looking at their cybersecurity posture and assessing its risk management maturity through a multi-discipline, consistent engagement, (vs. annual checklist-based approach) that aligns with established best practices, nationally recognized standards, and federal/international guidelines for cybersecurity. Through the cybersecurity risk assessment process and a "whole of community" approach, ports and facilities will foster cross-functional collaboration, promote awareness, and enhance communication and information sharing. Most importantly, this will become a continuous process that facilitates and fosters growth of cybersecurity and its resilience over time.

2 DIGITALIZATION

Ports and facilities will create and implement a Digital Twin, a full virtual representation of their physical footprint, for their facilities and associated critical infrastructure that they are responsible for protecting. This Digital Twin may be shared with the USCG as a planning tool, and can be used to reduce the cost of security compliance by automating tasks. Additionally, digitalization enhances the security of the port (or facility), local stakeholders, the port community, and the nation.

3 OPTIMIZATION

Leveraging the benefits of digitalization, ports and facilities will have tools to conduct continuous vulnerability assessments, for physical and cybersecurity, on a continual basis (vs one time every few years). Machine learning technology, that has been recognized by the Department of Defense, Department of Energy, and the Department of Homeland Security as a "best in class" tool, is applied to optimize the security posture of America's maritime critical infrastructure.

MARSEC Accreditation & Port Security Grant Program

GRANT ELIGIBILITY

4 TRAINING / EXERCISES

Ports and facilities will be advancing their workforce, through training tools that are in place and utilized to ensure regulatory compliance, and to expand the knowledge, skills, and awareness of their employees, contract security personnel, contractors, and other stakeholders. Ports and facilities have an opportunity to automate training and exercises tp save money. Additionally, digital tools facilitate adoption of new and modern methods of learning, enhancement, and engagement in order to shape future leaders in the maritime sector.

5 INTERCONNECTIVITY, INTELLIGENCE, AND INFO SHARING

Ports and facilities are connected in many aspects, through the Area Maritime Security Committees, regional intelligence centers, and through port and other maritime stakeholders locally and the nationwide. Using digital tools, threat intelligence information can be shared continually, and on a regular basis, among federal, state, and local entities, including direct communications with the USCG, and other key partners and national assets.

6 STRATEGIC PLANNING

Ports and facilities respond to incidents, and events in a pre-planned, well organized, and systemic process, which will be accentuated and enhanced through the implementation of digital tools, and MARSEC Accreditation.

MARSEC Accreditation addresses the National Preparedness Goal of: "[a] secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

Accreditation also directly addresses the National Preparedness Goal's Core Capability for Cybersecurity which, as stated, is to: "Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation."

MARSEC Accreditation meets FEMA's National Priorities for: Cybersecurity, Planning, Training and Exercises, and enhances Maritime Domain Awareness, Port Resilience and Recovery Capabilities, and Physical Security.