Maritime FSO Cybersecurity Training

Developed and Instructed by Experienced Maritime Cybersecurity Experts

In-person training course focused on cybersecurity fundamentals for Maritime Facility Security Officers (FSOs). Participants will be instructed on relevant regulatory requirements, such as those established by the Maritime Transportation Security Act (MTSA), the US Coast Guard and the International Maritime Organization (IMO). They will be introduced to fundamental concepts of IT and operational technology (OT) cybersecurity and industry standards such as those published by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the International Society of Automation (ISA) and the International Electrotechnical Committee (IEC).

Course participants will learn how to specify and commission a cyber security assessment and how to incorporate the findings into their existing facility security assessment (FSA). Likewise, they will learn how to interpret the findings from a cybersecurity assessment and use those to develop a cybersecurity plan that can be incorporated into the existing facility security plan (FSP).

Dates: May 25 & 26, 2021

4400 Highway 225
Suite 200
Deer Park, TX 77536

8:30 to 4:00 each day

Questions?
Contact Al Cusick 713-671-0947

Benefits of this course:

- Students will be provided with tools and templates they can immediately apply
- Students will learn cybersecurity principles and the “jargon” needed to communicate with internal and external cybersecurity consultants
- Students will be better prepared to specify the services required to meet the intent of the regulations and standards

Covered topics include:

- Computer and Network Systems
- Network Terminology and Concepts
- Cybersecurity Incidents and Impacts
- Maritime Transportation Security Regulations
- Maritime Cybersecurity Guidelines
- NIST Cybersecurity Guidelines
- ISA / IEC / ANSI Standards
- IT and OT Communications
- Asset Inventory
- Assessing and Managing Cybersecurity Risk
- Incident Response Planning (IRP) and Prevention
- Incident Management
- Post Incident Analysis and Forensics
- Patch Management
- Malware Management
- Access Control
- Remote Access
- Security Controls
- Backup and Restoration
- Documenting Vulnerabilities for Regulatory