“Cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my department and for our country’s security.”

Former DHS Secretary Nielsen
Emerging Technology / Increased Risks

Increasing Concern for Operational Technology (OT) Cybersecurity

Historically, OT systems were physically isolated from information technology (IT) networks, but the days of OT isolation are coming to an end. With the rise of technologies, such as Big Data, Data Analytics, and the Internet of Things, companies have increasing business needs to integrate OT with IT networks to remain competitive. This raises significant challenges to protect OT systems from exploitation.

IT/OT CYBERSECURITY

Information Technology creates, processes, stores, retrieves, & sends information. OT monitors & controls how physical devices perform their intended functions. IT & OT systems typically use different languages & protocols but share wiring infrastructure.

Consequences of System Exploitation

IT Financial Impacts
• Business interruption
• Sensitive data loss
• Reputational damage

OT Physical Impacts
• Deaths & injuries
• Property damage
• Environmental impacts

Opposite System Priorities

Highest
Confidentiality
Preserving authorized restrictions
Integrity
Performing its intended functions
Availability
Ensuring timely & reliable access

Marine Terminal

Landside Facility

External hackers can exploit systems remotely through the internet.

Simple local OT system controls bulk liquid transfers to/from ships.

Segmenting IT/OT into multiple functional zones is a best practice.

Insider threats can exploit well-segmented OT systems through direct physical access.

IT cybersecurity is governed at the corporate level with programs designed to protect, detect, respond, and recover from intrusions.
• Coast Guard Cyber Strategy (June 2015)

- Strategic Priorities:

1. Defending Cyberspace
2. Enabling Operations
3. Protecting Infrastructure
Cyber Risk Awareness

1) Conduct a Risk Assessment
2) Identify or Adopt Best Practices
3) Secure the Supply Chain
4) Measure Progress
5) Revise and Improve Security
Cyber Risk Management

- **CG-5P Policy Letter 08-16**
  - Reporting Suspicious Activity & Breaches of Security

  - Criteria for reporting BoS and/or SA for both physical & cyber related events
  - SA: Large, sustained cyber attacks in an apparent attempt to exploit them
  - Reports to the NRC
  - National Cybersecurity & Communications Integration Center (NCCIC)
    - Cyber incidents only, do not involve physical or pollution effects
Cyber NVIC

- Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities
  - Guidance on incorporating computer systems & networks into FSAs & FSPs
  - Clarifies 33 CFR 105 & 106
  - 250+ comments on draft NVIC
  - Currently under review
TWIC

- TSA began issuing new TWIC cards on July 10, 2018 with enhanced efforts to combat counterfeiting
TWIC Authentication Features

The TWIC card maintains several overt design features to promote secure use of the credential.

1. Frontal facial photograph of the card holder.
2. Credential Expiration Date: Color-coded background that will update on annual basis.
3. Card Holder’s Full Name: last name, first name, and abbreviated middle name (first initial followed by period) in capital letters.
4. Color Shifting Ink: TWIC text and Propeller design color shifts between red, gold, and green (depending on lighting conditions) when viewed from different angles.
5. Tactility: Card Identification Number (CIN) and Anchor design embossed on the card’s laminate. (The CIN is an 8 digit number that can be validated to the CIN printed on the rear of the card, bottom left.)
6. Image Transition Effect: Compass changes to U.S. Flag design when viewed from different angles. (Laminate)
7. Letter Lenses: T, W, L, and C letters visible within circle designs using LED light source. (Laminate)
8. Kinetic Image: Rope design color changes when viewed from different angles. (Laminate)
9. Image Glint/Reflection: Anchor image visible within Compass design using LED light source. (Laminate)
10. Shaped Lenses/Images: Star designs partially covering photograph with color changes when viewed from different angles. (Laminate)

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity’s security office for more information.

For more information on the TWIC card, please contact TSA at: twic.issue@tsa.dhs.gov.
TWIC Reader Rule

• Transportation Worker Identification Credential Accountability Act signed into law August 2, 2018
• Prohibited CG from requiring electronic inspections of TWIC cards until after the Department of Homeland Security submitted an assessment of the TWIC program to Congress
• DHS assessment results awaiting Congressional review
Seafarers’ Access

• Regulated facilities to provide a system for seafarers assigned to a vessel at that facility, pilots, and representatives of seafarers’ welfare and labor organizations to board and depart the vessel through the facility in a timely manner and at no cost to the individual.

• Feb 3, 2020: facility must submit an amendment to FSP describing how it will meet the regulation

• June 1, 2020: system must be in place
Facility Compliance

Common Deficiencies:

- Recordkeeping/documentation
- Facility signage
- Hose markings
- Secondary containment

Deficiencies Trending Down

- 2017
- 2018
- 2019

# Deficiencies
Cyber Awareness Training

- 101 level awareness training for familiarity of cyber terms/issues in MTS
- Tailored to AMSC audience in the form of a webinar
- Available for all audiences