

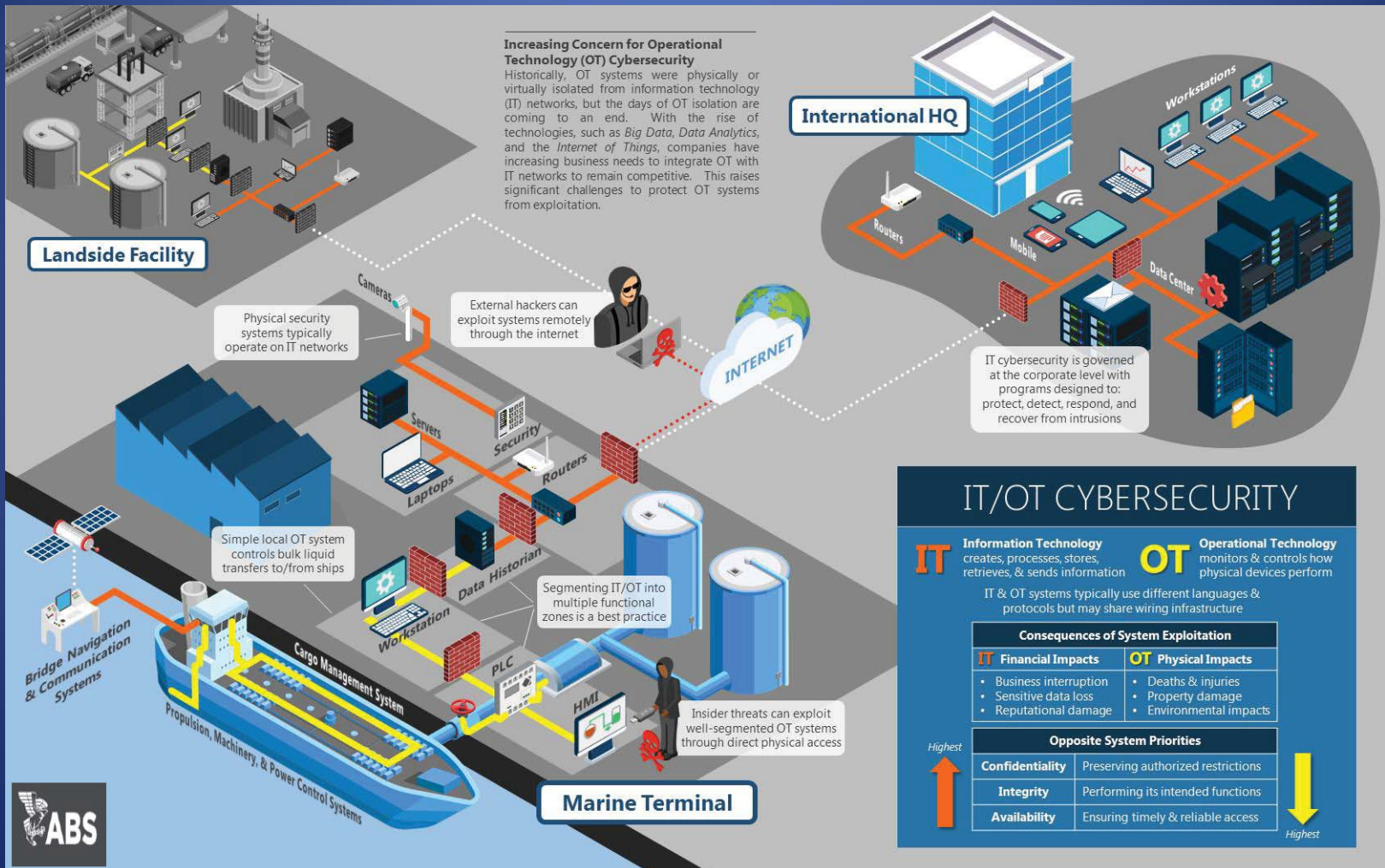
Cyber Risk Management

“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



IT/OT CYBERSECURITY

IT Information Technology creates, processes, stores, retrieves, & sends information

OT Operational Technology monitors & controls how physical devices perform

IT & OT systems typically use different languages & protocols but may share wiring infrastructure

Consequences of System Exploitation	
IT Financial Impacts	OT Physical Impacts
<ul style="list-style-type: none"> Business interruption Sensitive data loss Reputational damage 	<ul style="list-style-type: none"> Deaths & injuries Property damage Environmental impacts

Opposite System Priorities

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

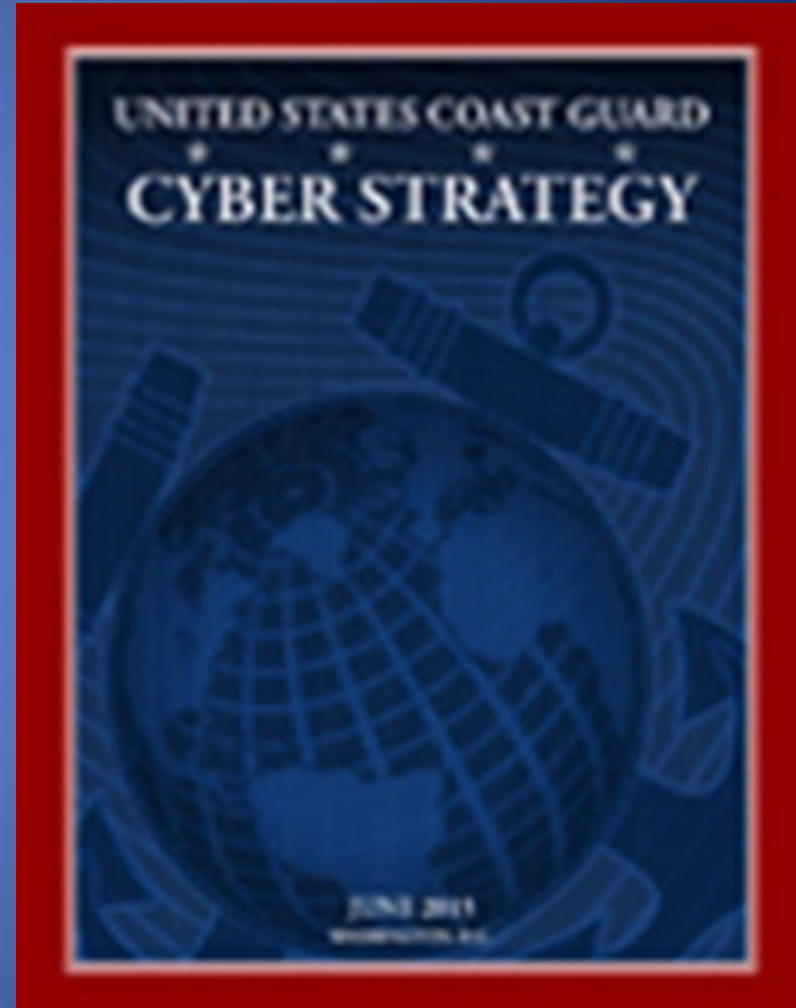


Cyber Risk Management

- **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

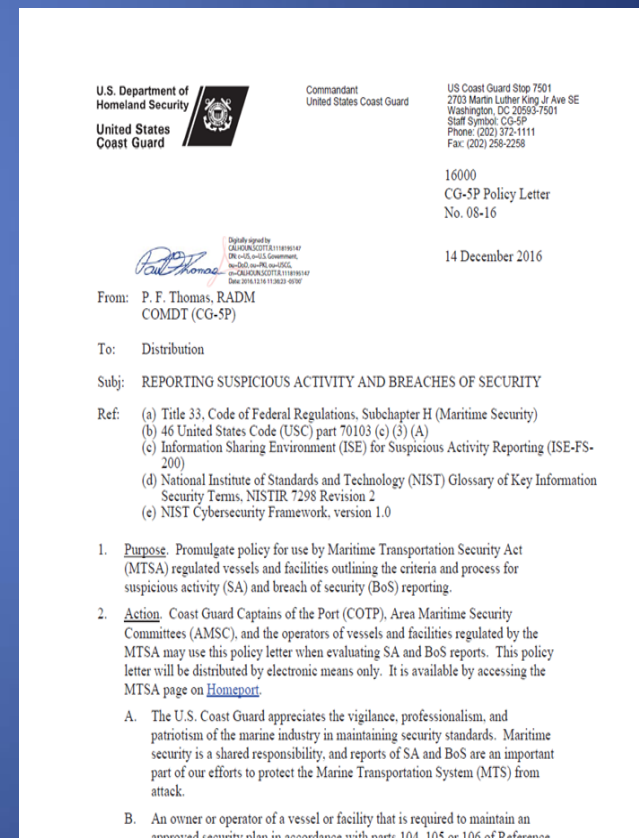


Cyber Risk Management

- **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

U.S. Department of Homeland Security
United States Coast Guard



Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20593-7501
Staff Symbol: CG-5P

COMDTPUB xxxxxxxx
NVIC 05-17

DRAFT NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 05-17

Subj: GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES

Ref: (a) Title 33 of the Code of Federal Regulations (CFR) Subchapter H, Maritime Security
(b) National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF)

1. **PURPOSE.** In accordance with 33 CFR parts 105 and 106, MTSA-regulated facilities are instructed to analyze vulnerabilities with computer systems and networks in their Facility Security Assessment (FSA). This Navigation and Vessel Inspection Circular (NVIC) will assist Facility Security Officers (FSOs) in completing this requirement. Additionally, this NVIC provides guidance and recommended practices for Maritime Transportation Security Act (MTSA) regulated facilities to address cyber related vulnerabilities. Until specific cyber risk management regulations are promulgated, facility operators may use this document as guidance to develop and implement measures and activities for effective self governance of cyber vulnerabilities.

2. **ACTION.**

Enclosure (1) provides draft interpretive guidance regarding existing regulatory requirements in 33 CFR parts 105 and 106, which instruct facilities to conduct FSAs and address any vulnerabilities identified in the FSA in the Facility Security Plan (FSP). This guidance would detail how those existing requirements relate to cybersecurity measures, and what would be recommended to be included in the FSP.

Enclosure (2) provides draft guidance on implementing a cyber risk management governance program to include establishment of a cyber risk management team, policies, programs, and identification of critical systems. This guidance is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82, and provides more detail regarding the development of a Cyber Risk Management Program (CRMP) and specific examples as to how such a program can be implemented in a variety of system and business configurations.

Appendix (A) contains the tables referred to in Enclosure (2).



TWIC

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



TWIC



Transportation Worker Identification Credential

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 shift 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, I, 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. Shape 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



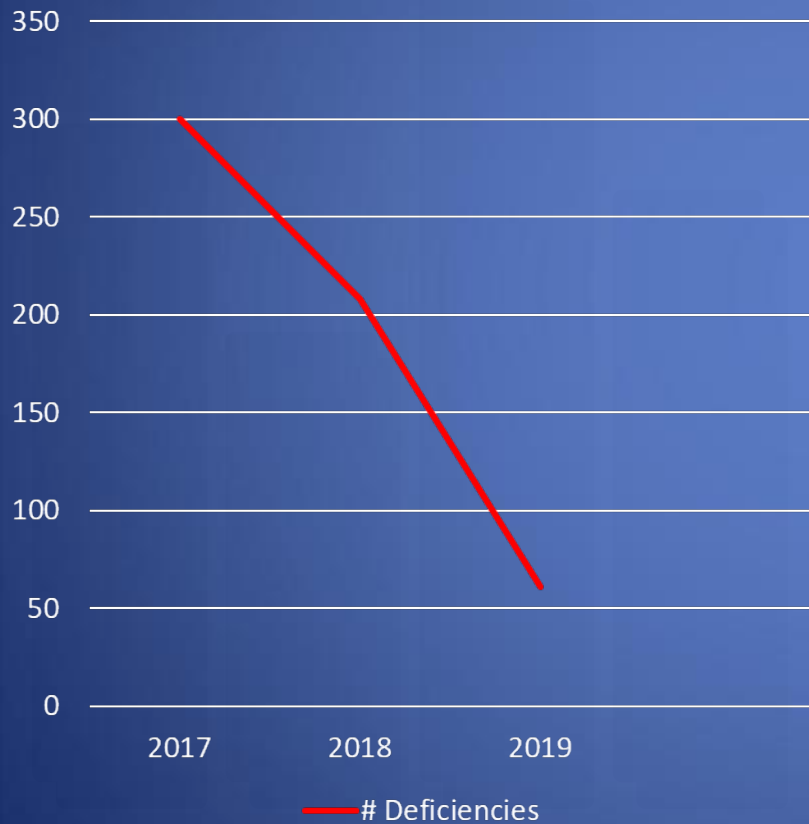
Seafarers' Access

- 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

Deficiencies Trending Down



Common Deficiencies:

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



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
- USCG Domestic Ports Division Security Website:
(<https://www.dco.uscg.mil/Portals/9/CG-FAC/Videos/Maritime%20Cybersecurity%20Awareness%20-%20May%2016%202018.mp4?ver=2018-05-25-083330-703>)

Maritime Cybersecurity Awareness

Cris DeWitt

Senior Technical Advisor, ABS Advanced Solutions

cdewitt@eagle.org

Matt Mowrer

Director of Applied Technology & Data Analytics

mmowrer@abs-group.com



© 2017 ABS Group of Companies, Inc. All rights reserved.

