



Understanding Cyber Security Through the Lens of USCG NVIC 01-20

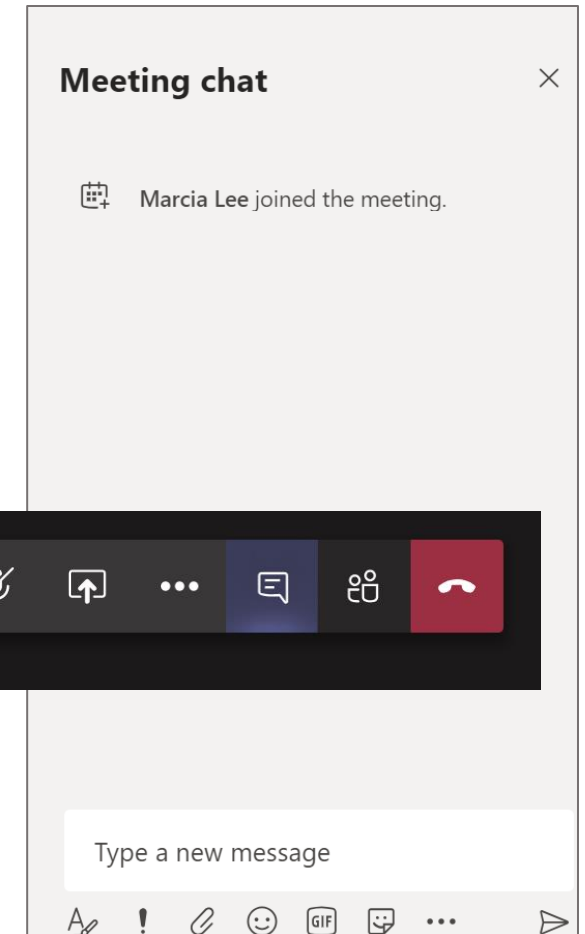
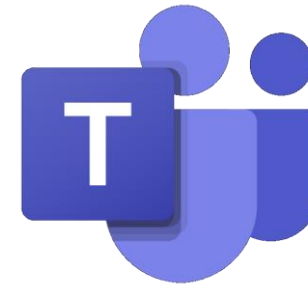
Dennis Hackney – Head of Cyber Solutions, ABSG
Marcia Lee – Manager, Business Development, ABSG

Questions

- Enter your question(s) in the Teams Chat section at this time.
- Today's webinar is being recorded and will become available at: www.abs-group.com/webinars
- Please allow 1-2 business days for the webinar recording to be posted.

Reminder: Do not discuss Sensitive Security Information (SSI) specific to your facility in the questions.

Ref: 49 CFR 1520



Agenda

- Safety Moment
- Real World Incidents
- Facility Cyber Security Challenges
- NVIC 01-20 Overview
- Correlating NVIC 01-20 to 33 CFR 105 and 106
- MSIB and CISA Alert Recommendations
- Cyber TSI
- NVIC 01-20 Guidelines
- FSO's Cyber Role
- Incident Command System and Facility Cyber



Safety Moment – COVID-19

- Work from home requirements
- Remote access
- Is your facility ensuring your access into facility's systems is remotely secured?
- Stay vigilant with passwords



Safety Moment – COVID-19

- Malicious actors are now looking to steal critical data from your work
- Phishing increasingly utilized:
 - Phone scams
 - E-mails claiming to be government announcements
 - Online meeting hijacking
 - Financial theft
- How much identifying information do you have published on your company's website?

Cyber Attack Disrupts COVID-19 Payouts: Hackers Take Down Italian Social Security Site

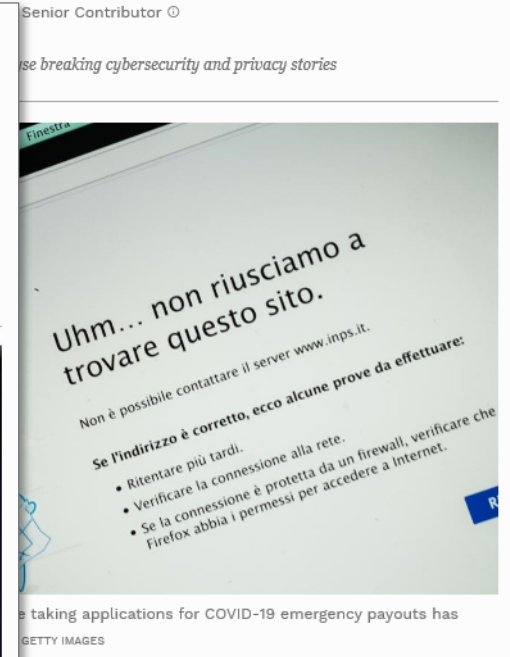
Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails



Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.



Computer viruses are likely to spread as malicious hackers make the most of the COVID-19 panic. ... [+] SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES



Source: Forbes.com

Real World Incidents



Attackers are rapidly evolving their tactics as they learn more about the environment

Disrupting, delaying or destroying critical infrastructure and assets is a major incentive

There are a variety of attackers

- Examples: Nation states, organized crime, terrorist, hackers

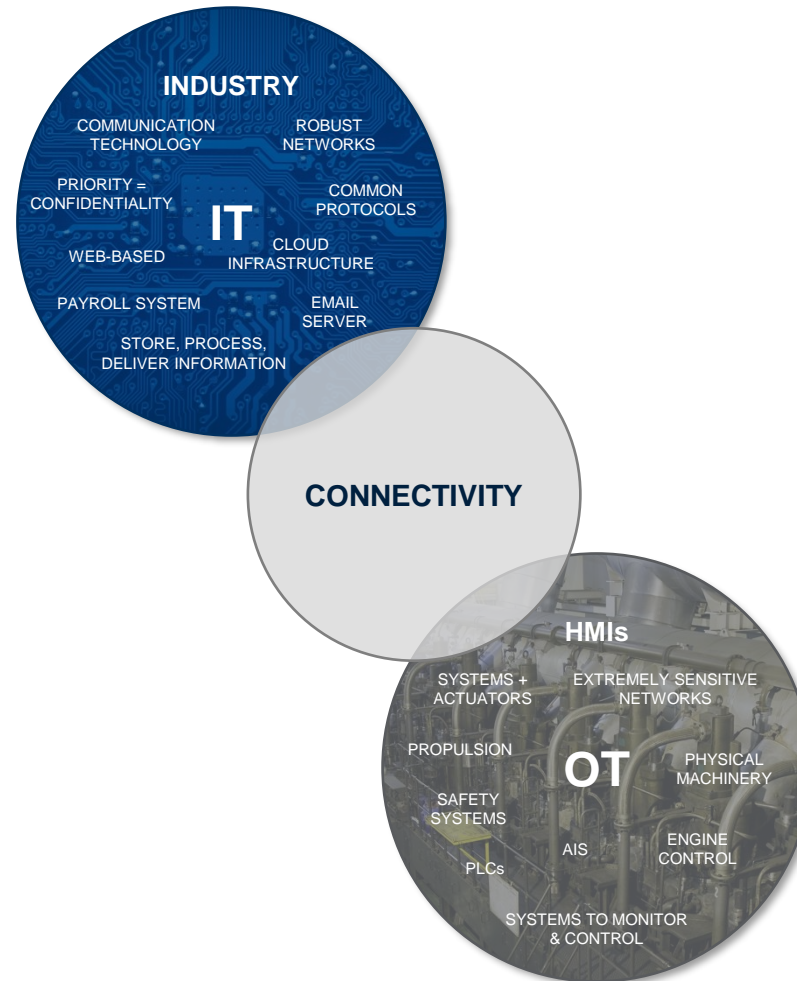
Attacks have grown in frequency and intensity

- Examples: Ransomware, insider threat, phishing attacks, malware, zero day

OT Security: The problem is getting easier to see

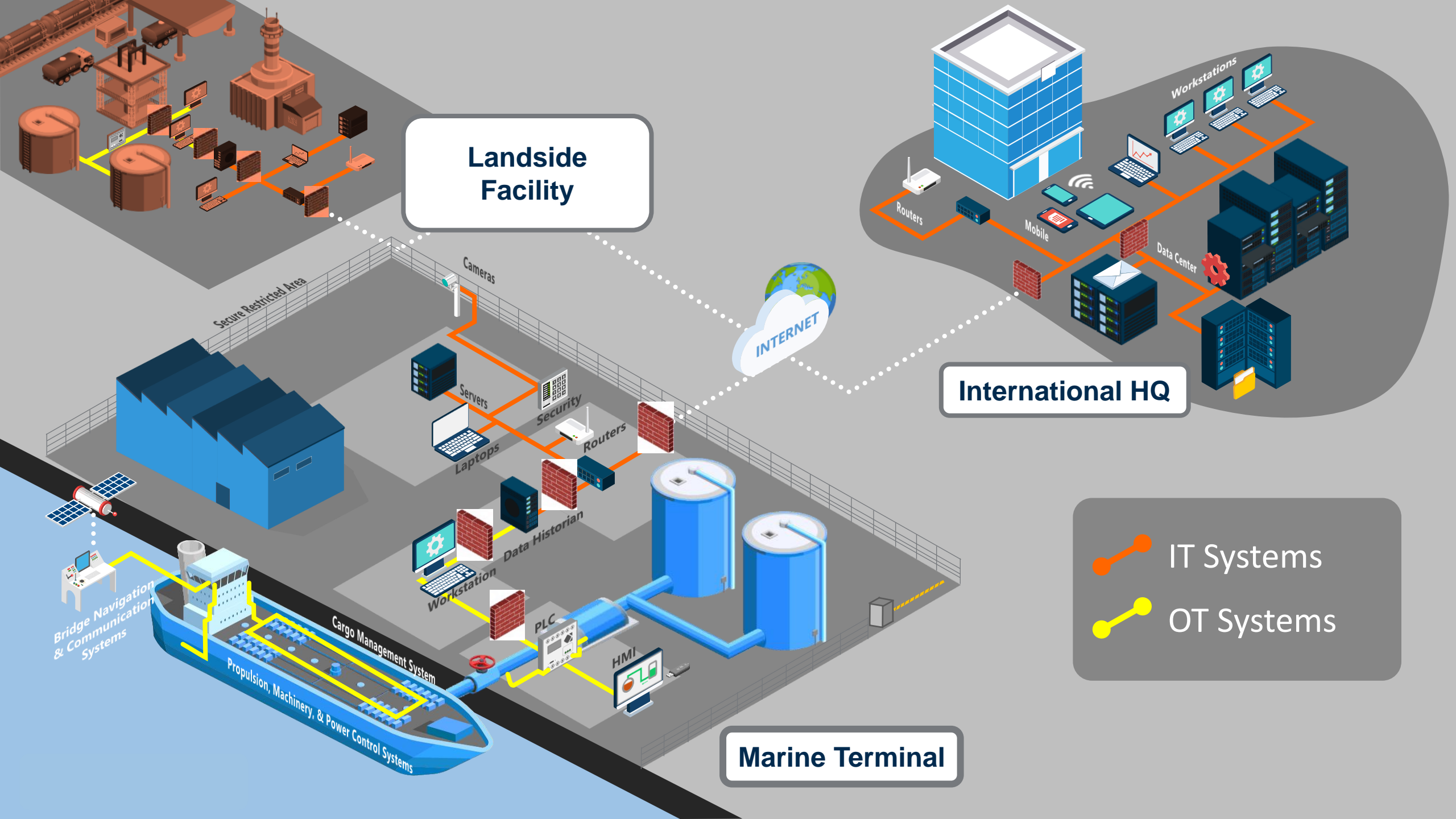
Information Technology (IT)

- Lifecycle management
 - Component lifetime: 2-5 years
 - Upgrades are straightforward and changes are automated
- User expectations
 - High throughput demanded
 - High delay is accepted
 - Data security is essential
- Cyber Security
 - Primary concern: Loss of data
 - Mature practices and high awareness



Operational Technology (OT)

- Lifecycle management
 - Component lifetime: 10-20 years
 - Changes require specialized personnel and careful planning
- User Expectations
 - Moderate throughput acceptable
 - High delay is a serious impact
 - Fault tolerance and redundancy essential
- Cyber Security
 - Loss of life, environmental damage, equipment damage
 - Ad hoc or no processes and lack of awareness



Landside Facility

International HQ

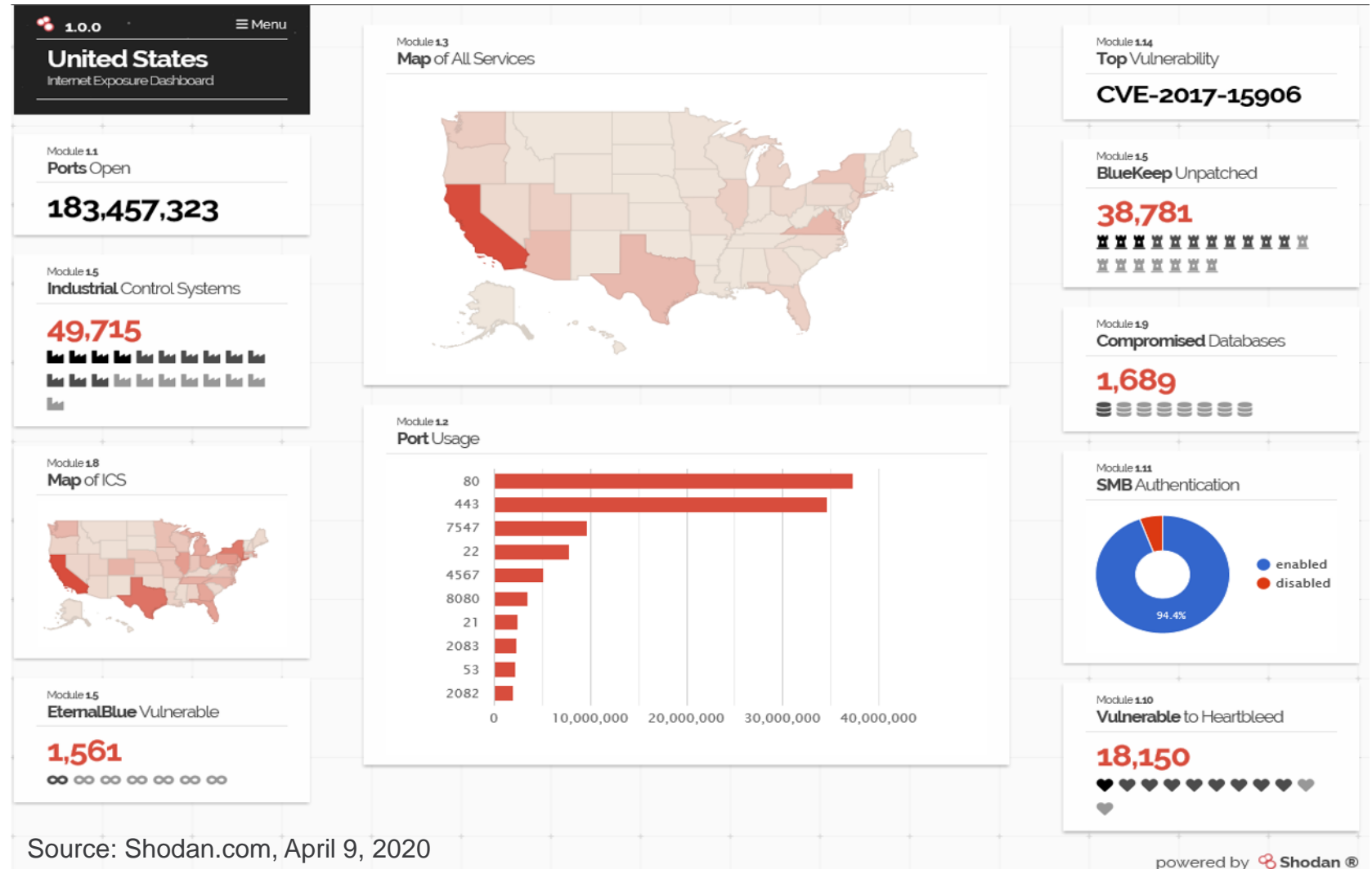
Marine Terminal

- IT Systems
- OT Systems

Here's the Problem...

Industrial Control Systems are Vulnerable

- Easy Access to Unprotected ICS



USCG Cyber Guidance: USCG NVIC 01-20 ➔ NIST CSF



U.S Coast Guard
Navigation and
Vessel Inspection
Circular 01-20
(USCG NVIC 01-20)

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

Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20568-7818
Staff Symbol: CG-FAC
Phone: (202) 372-1107

COMDTPUB P16700.4
NVIC 01-20
February 26, 2020

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 01-20

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

1. **PURPOSE.** This Navigation and Vessel Inspection Circular (NVIC) provides guidance to facility owners and operators in complying with the requirements to assess, document, and address computer system or network vulnerabilities. In accordance with 33 CFR parts 105 and 106, which implement the Maritime Transportation Security Act (MTSA) of 2002, as codified in 46 U.S.C. Chapter 701, regulated facilities (including Outer Continental Shelf facilities) are required to assess and document vulnerabilities associated with their computer systems and networks in a Facility Security Assessment (FSA). If vulnerabilities are identified, the applicable sections of the Facility Security Plan (FSP) must address the vulnerabilities in accordance with 33 CFR 105.400 and 106.400.

2. **DISCLAIMER.** This NVIC is intended only to provide clarity regarding existing requirements under the law. It does not change any legal requirements, and does not impose new requirements on the public. Not all recommendations will apply to all facilities, depending on individual facility operations. Facility owners and operators may use a different approach that has greater or lesser complexity than this NVIC recommends, if that approach satisfies the applicable legal requirements (*i.e.*, this NVIC does not represent a minimum requirement for compliance).

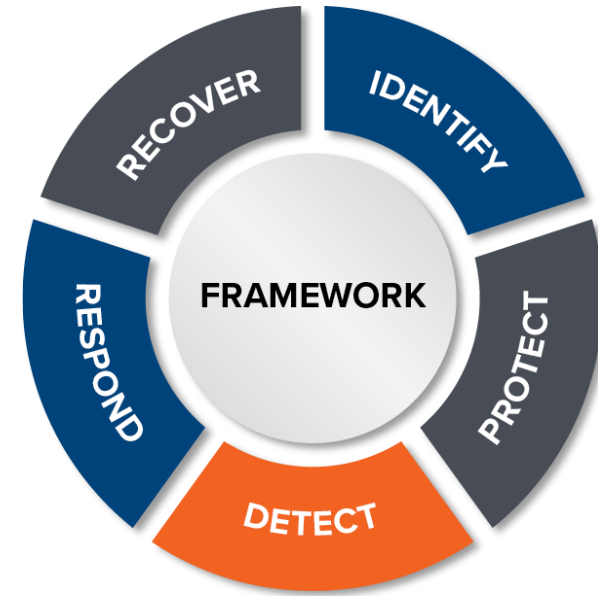
3. **ACTION.**

a. Enclosure (1) provides a list of existing MTSA regulatory requirements that may apply once a facility owner or operator identifies computer system and/or network vulnerabilities

DISTRIBUTION - SOL No. 170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	X	X	X	X											X										X	
B																										X
C																										
D				X						X																
E				X										X			X									
F																										
G																										
H							X			X																

NON-STANDARD DISTRIBUTION



NIST Cyber Security Framework

- **NIST SP 800-53, Rev 4** – Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-82, Rev 2** – Guide to Industrial Control Systems (ICS) Security

Connecting the Dots



USCG NVIC 01-20 Standards

1 Facility Security Assessments

2 Security Administration and Organization

3 Personnel Training

4 Drills and Exercises

5 Records and Documentation

6 Response to Change in MARSEC Level

7 Communications

8 Procedures for Interfacing with Vessels

9 Security Measures for Access Control

10 Security Systems and Equipment Maintenance

11 Security Measures for Restricted Areas

12 Security Measures for Handling Cargo

13 Security Measures for Delivery of Stores

14 Security Measures for Monitoring

15 Facility Security Plan – Cyber Annex

16 Audits and Security Plan Amendments

MSIB 18 – 20 and CISA Alert



Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr. Ave. SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 18-20
Date: July 24, 2020
Contact: Brandon Link, CDR
Phone: (202) 372-1107
E-Mail: brandon.m.link@uscg.mil

URGENT NEED TO PROTECT OPERATIONAL TECHNOLOGIES AND CONTROL SYSTEMS

The cyber landscape in the Marine Transportation System (MTS) is continually evolving. Computer systems and technology play an increasing role in systems, and while advances in systems and technologies can heighten the risk of increased threats posed by an unwillingness to conduct malevolent activity against operational technology (OT) assets.

Internet-accessible OT assets are prevalent across not designed to defend against current threats as protect newer systems and equipment, create of maritime operations lends itself to interactions necessitating a continually increasing focus on

The Cybersecurity and Infrastructure Security Agency's [Immediate Actions to Reduce Exposure Across](#) relevant to the MTS. The maritime sector heavy recommendations in it can help reduce cyber risk

The Coast Guard continues to work with mariners best practices. Recently released policy include [Guidelines for Addressing Cyber Risks at Mar](#). This NVIC provides guidance to Maritime Transporting with requirements to assess, document. Additionally, a [Facility Inspector Cyber Job Aid](#) with additional guidance as they address facilities may likewise reference this guide for additional

As always, any potential threat to the cybersecurity of Security or Suspicious Activities Response Center at 1-800-424-8802. For additional Command's 24x7 watch at 202-372-3904 or via willingness to comply and report in a timely manner maritime critical infrastructure safer.

Richard V. Timme, RDML, U. S. Coast Guard

MSIB 18-20



NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems

Summary

Over recent months, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets [1]. Due to the increase in adversary capabilities and activity, the criticality to U.S. national security and way of life, and the vulnerability of OT systems, civilian infrastructure makes attractive targets for foreign powers attempting to do harm to US interests or retaliate for perceived US aggression. OT assets are critical to the Department of Defense (DoD) mission and underpin essential National Security Systems (NSS) and services, as well as the Defense Industrial Base (DIB) and other critical infrastructure. At this time of heightened tensions, it is critical that asset owners and operators of critical infrastructure take the following immediate steps to ensure resilience and safety of US systems should a time of crisis emerge in the near term. The National Security Agency along with the Cybersecurity and Infrastructure Security Agency recommend that all DoD, NSS, DIB, and U.S. Critical Infrastructure facilities take immediate actions to secure their OT assets.

Internet-accessible OT assets are becoming more prevalent across operations and monitoring, accommodate a decentralized workforce Instrumentation & Control, OT asset management/maintenance, and maintenance. Legacy OT assets that were not designed to defend a readily available information that identifies OT assets connected via creating a "perfect storm" of 1) easy access to unsecured assets, 2) devices, and 3) an extensive list of exploits deployable via common Impact [6], and Immunity Canvas [7]. Observed cyber threat activity Tactics, Techniques, and Common Knowledge (ATT&CK) for Industrial important to note that while the behavior may not be technically advanced impact to critical assets is so high.

Recently Observed Tactics, Techniques, and Procedures

- Spear phishing [T1192] to obtain initial access to the organization pivoting to the OT network.
- Deployment of commodity ransomware to Encrypt Data for Connecting to Internet Accessible PLCs [T883] requiring no
- Utilizing Commonly Used Ports [T885] and Standard Application controllers and download modified control logic.
- Use of vendor engineering software and Program Download
- Modifying Control Logic [T833] and Parameters [T836] on P

CISA Alert (AA20-205A)

NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems

Recommended Mitigations from CISA include:

1. Have a Resilience Plan for OT
2. Exercise your Incident Response Plan
3. Harden Your Network
4. Create an Accurate "As-operated" OT Network Map Immediately
5. Understand and Evaluate Cyber-risk on "As-operated" OT Assets
6. Implement a Continuous and Vigilant System Monitoring Program



CISA Cybersecurity Practices for Industrial Control Systems

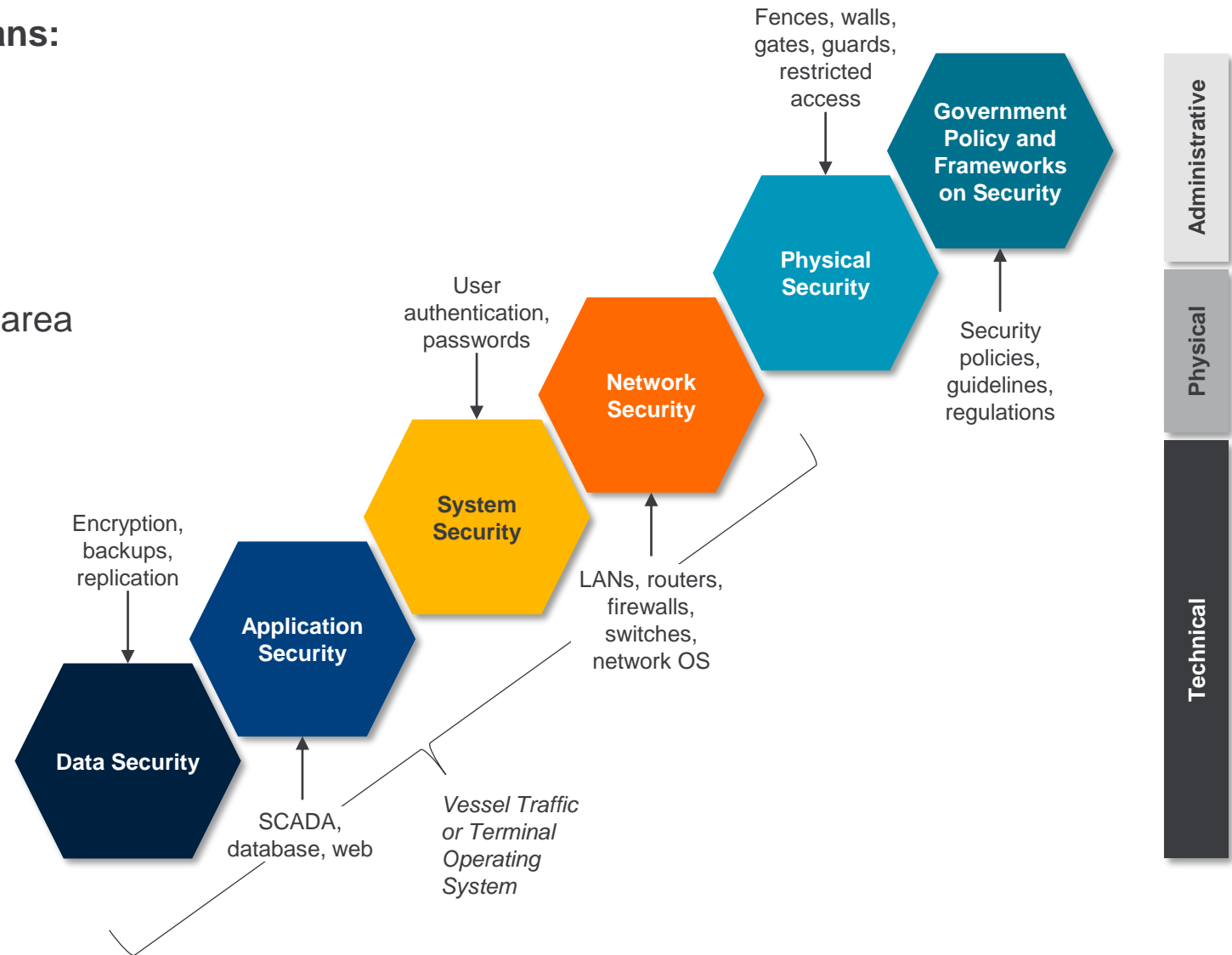
Transportation Security Incident and Cyber Security

Transportation Security Incident (TSI) means:

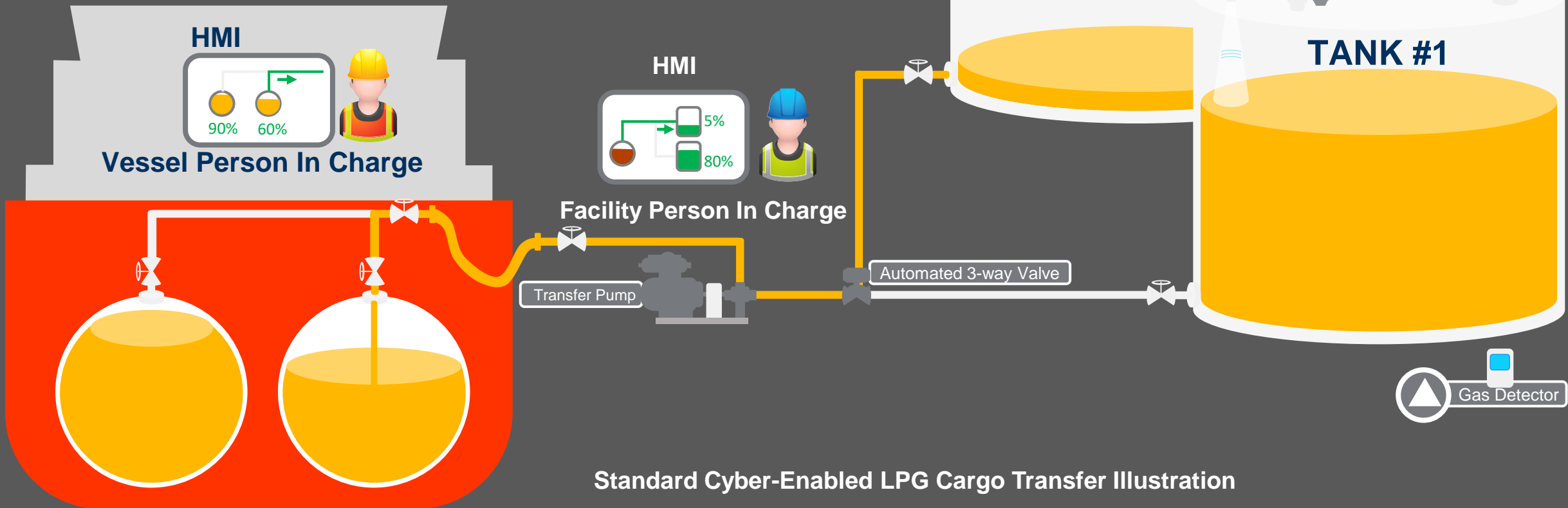
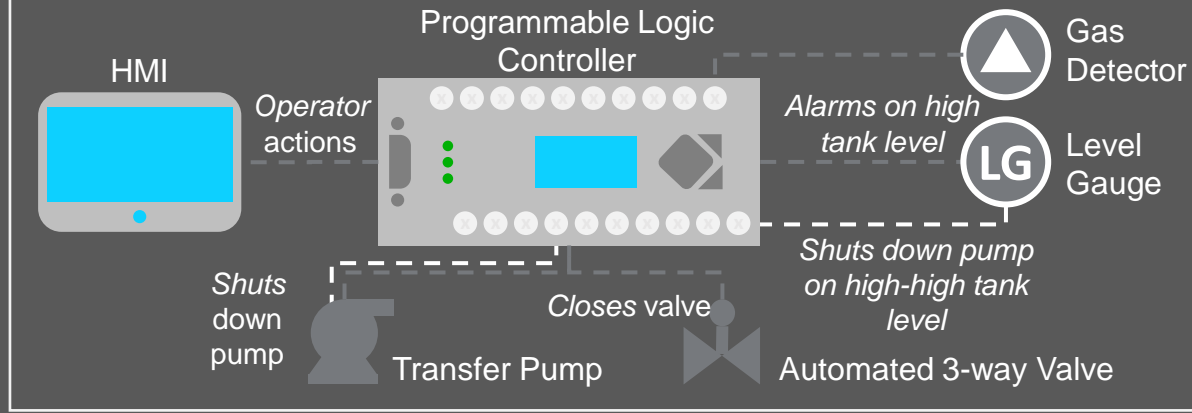
A security incident resulting in:

- a significant loss of life,
- environmental damage,
- transportation system disruption,
- or economic disruption in a particular area

Captain of the Port (COTP) has discretion

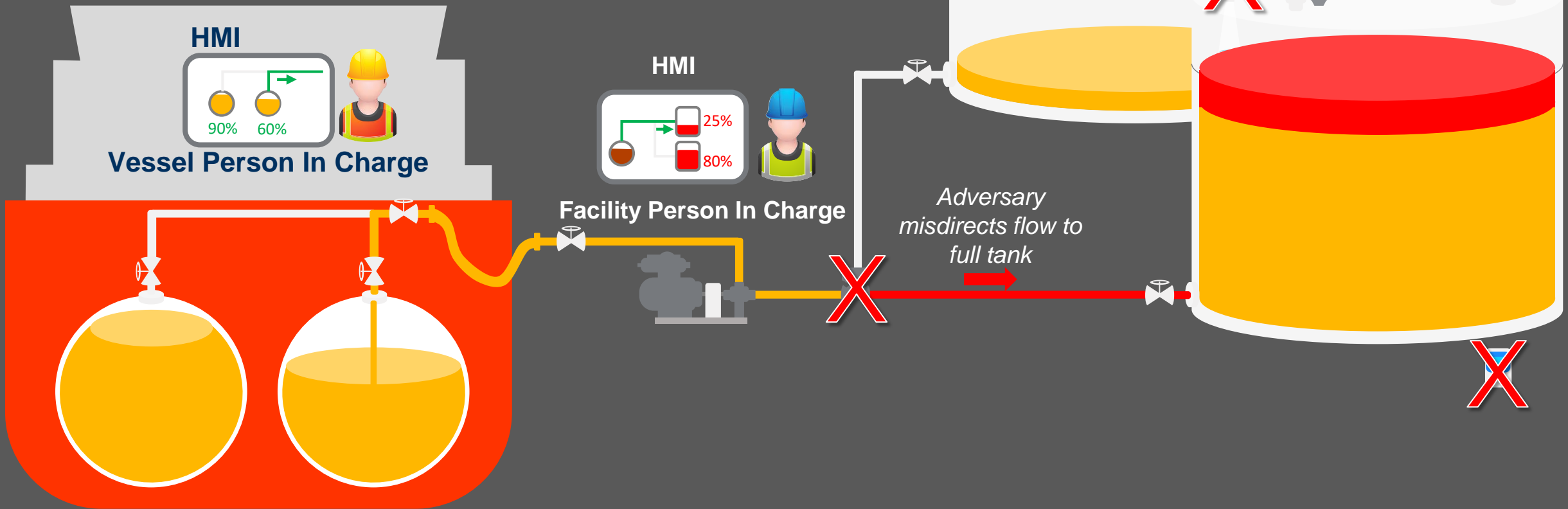
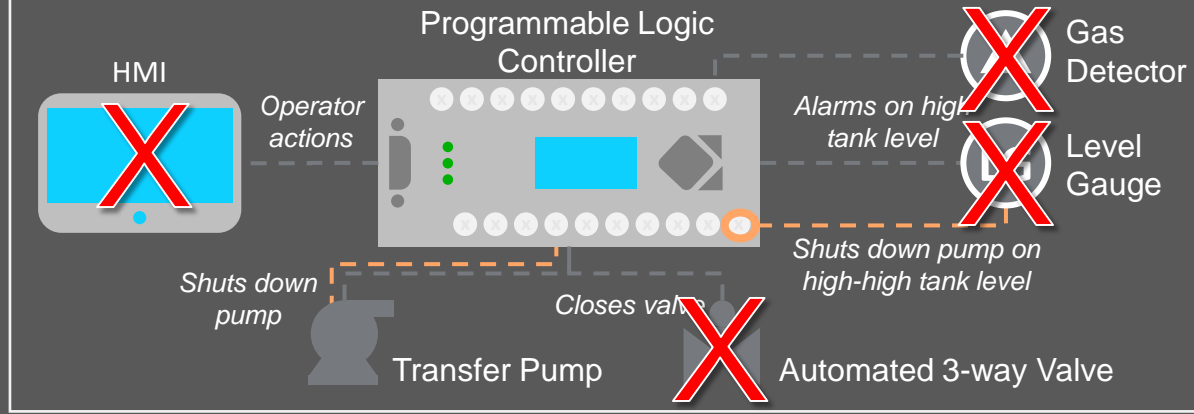


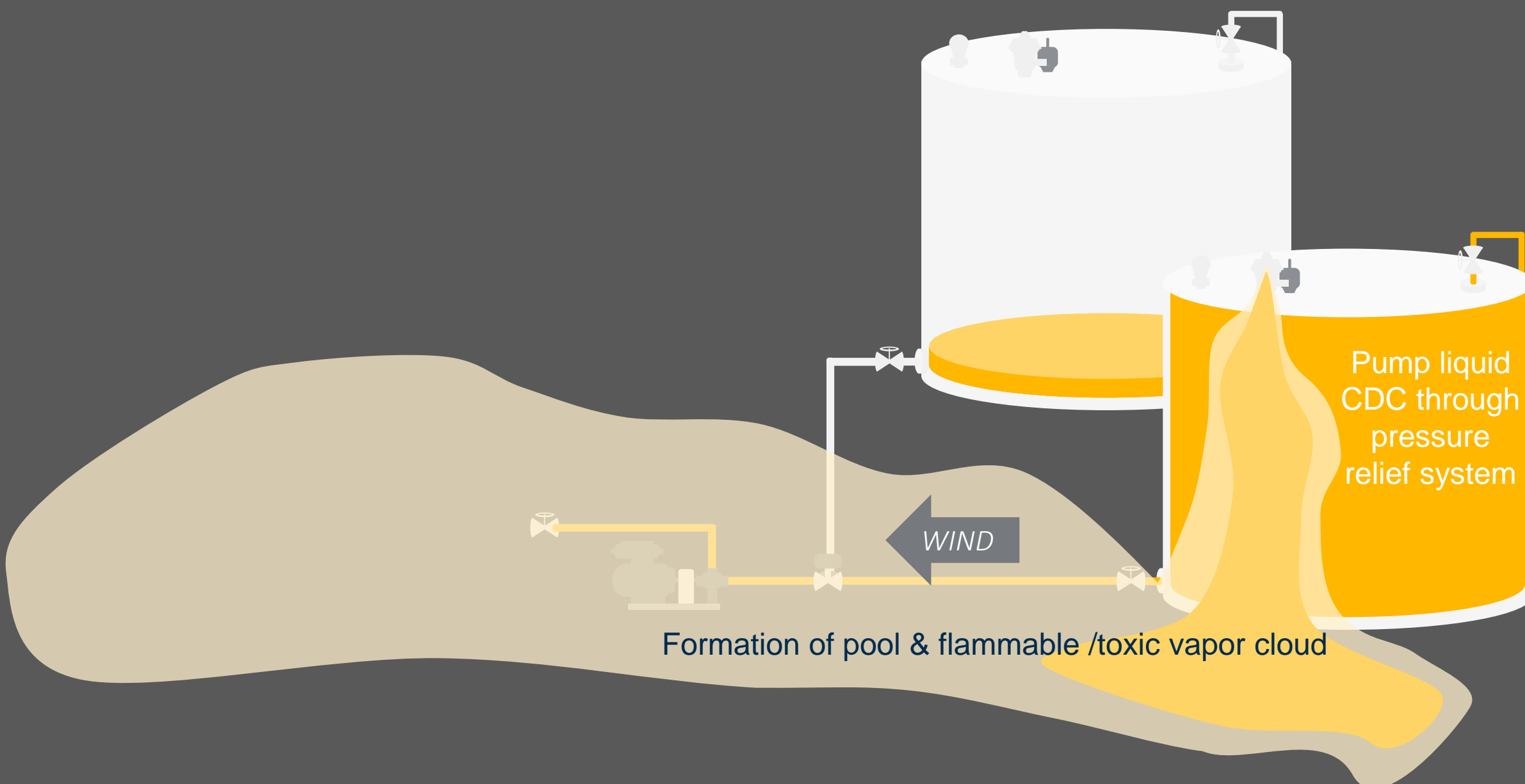
FACILITY ICS ARCHITECTURE



Standard Cyber-Enabled LPG Cargo Transfer Illustration

FACILITY ICS ARCHITECTURE



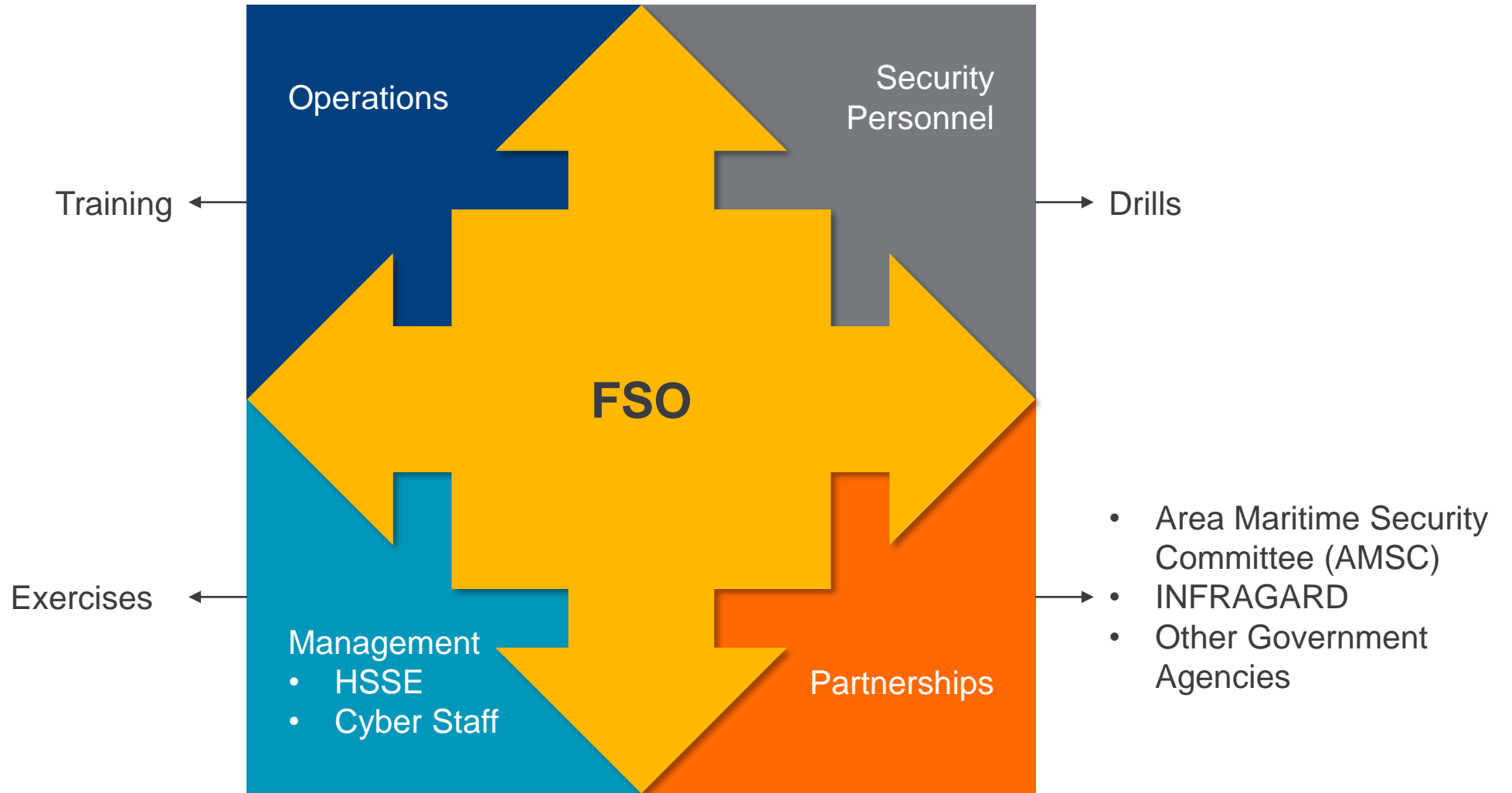


Pump liquid
CDC through
pressure
relief system

WIND

Formation of pool & flammable /toxic vapor cloud

Facility Security Officer Cyber Square



Facility Security Assessments – Cyber

- Cyber assessment should be treated the same as physical security assessments
- Important for the assessor to combine physical aspects
- Recommended stakeholder participation
 - FSO
 - AFSSO
 - IT
 - OT
 - Operations Staff
 - Management
 - HSSE/SHE Manager



Facility Security Plan – Cyber Annex

- **Highly discourage writing cyber security measures DIRECTLY into FSP**
 - FSP holds you accountable if something goes wrong
- **Create a separate cyber security plan or annex**
 - Address each cyber vulnerability identified in the FSA
 - Incident response
 - Incorporate ICS



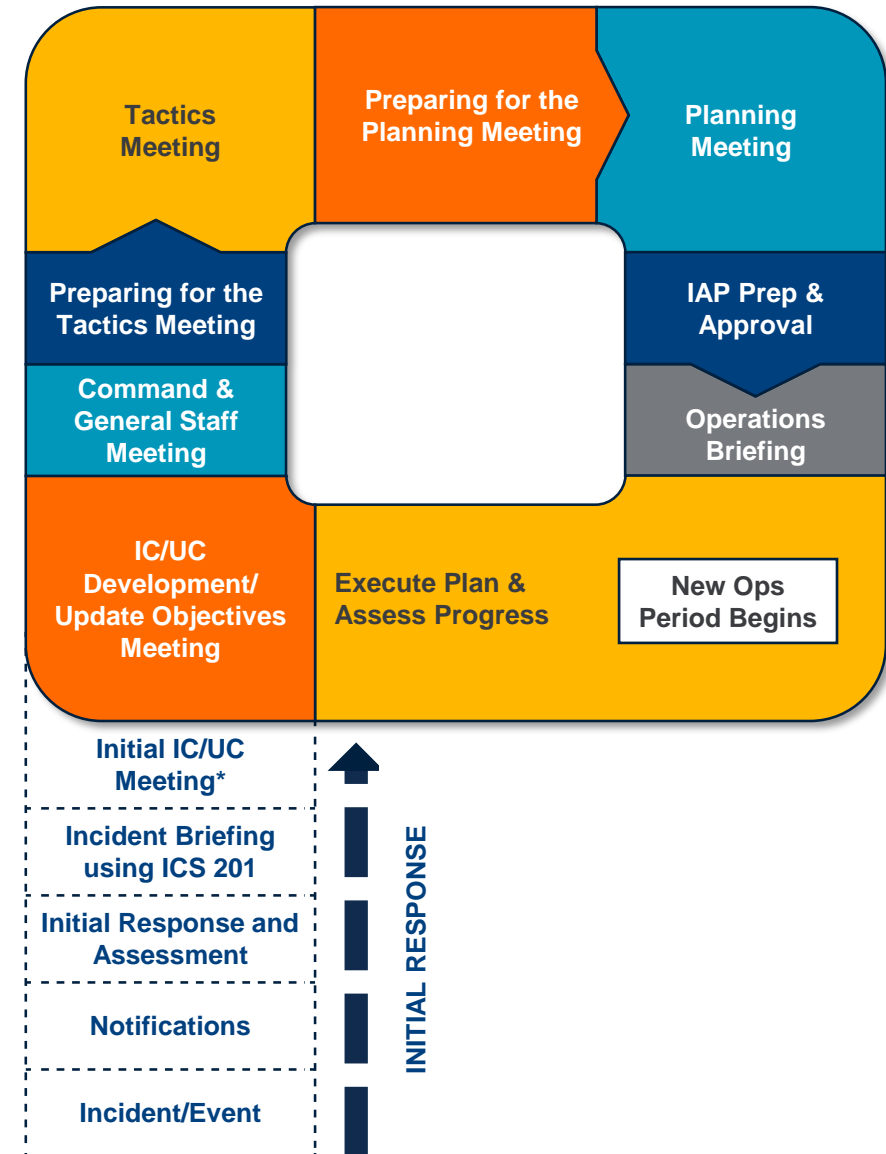
Drills / Exercises

- Enhances response capabilities
- Bridge the gap between FSOs and Cyber staff
- Raise awareness/builds culture
- **Combine physical-cyber scenarios**
- Recommend Incident Command System (ICS)

Date and time of drill/incident:
Scenario: A facility network administrator, who has been disgruntled throughout the past several months, is tasked with installing a patch upgrade. The individual is scheduled to leave that afternoon for vacation and as a result, installs the patch in a hurry. Later that afternoon, no one can login to their account and IT staff have discovered that the patch was installed with no testing. Inject: A facility employee overheard the individual state that they would covertly seek revenge against the facility for a formal reprimand they received earlier in the year.
Personnel Present:
Actions taken:
Notifications made:
Lessons learned to improve Cyber Security Plan and the FSP:

Incident Command System – Cyber

- Facility personnel should be using the Incident Command System (ICS) for cyber response
- Include as part of drills and exercises
- Combine with existing physical and weather threats
- Team with other facilities, AMSC members, or other government agencies
- Tie cyber into your facility Emergency Response Plan (ERP)



Beyond the Requirement...

- Preserve your facilities' reputation
- Foster safety into your cyber program
- Although implementation is not required until Sep. 30, 2021, early adopters will benefit from it
 - Short term – reduces the likelihood of a cyber incident
 - Long term – prepares you to exceed the expected standards outlined in USCG NVIC 01-20
- In NVIC 01-20, the Coast Guard makes very clear that performing cyber security assessments and addressing cyber security in FSP is a requirement.
- **Implementing Cyber Risk Management will put you in a better position to be more competitive.**






Dennis Hackney, PhD, CISSP

Head of Cybersecurity Solutions Development
DHackney@absconsulting.com

Marcia Lee

Manager, Business Development
MLee@absconsulting.com

 [linkedin.com/company/absgroup](https://www.linkedin.com/company/absgroup)

 @_absgroup

