ABS Group

AMERICA'S BEST MANAGEMENT CONSULTING FIRMS

Forbes 2021

POWERED BY STATISTA

Complying with U.S. Coast Guard Regulations

For MTSA-Regulated Facilities

Marcia Lee – Manager, Business Development

Brian Shajari – Senior Cybersecurity Assessor

ABS Group

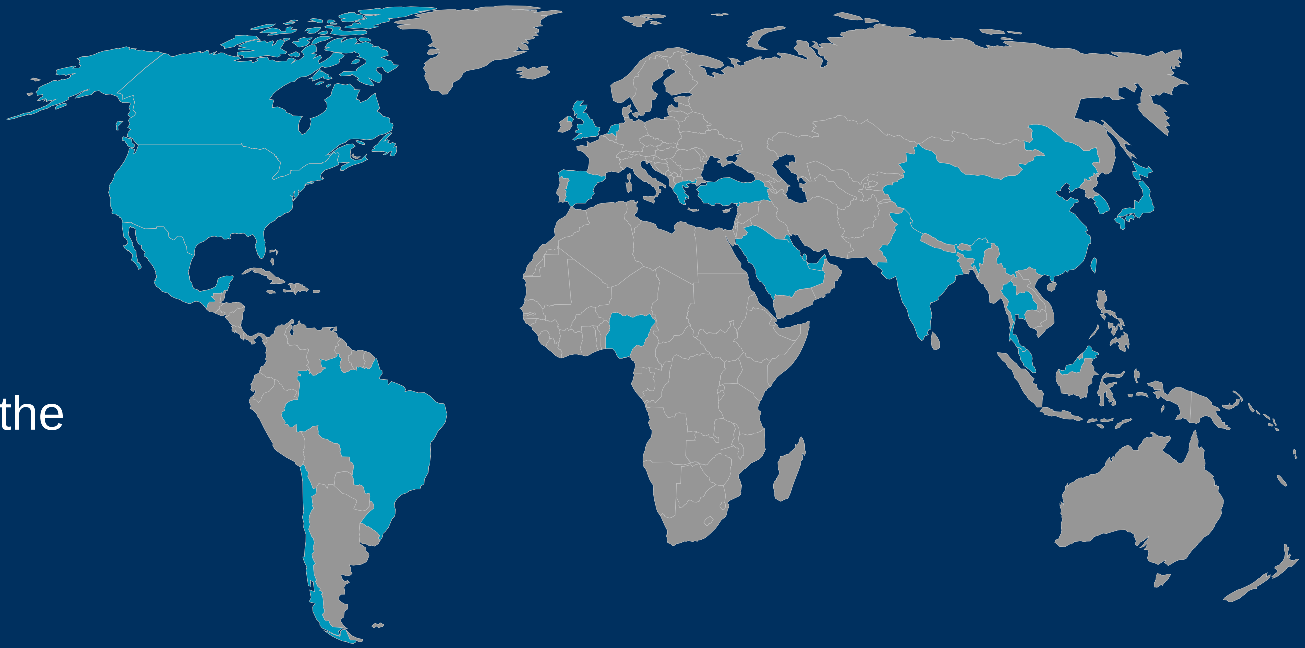
ABS Group provides data-driven risk and reliability solutions and technical services that help clients confirm the safety, integrity, quality and environmental efficiency of critical assets and operations.

ABS Group is focused on adding value to the industries served and strategically capturing synergies with the American Bureau of Shipping (ABS).

1000+ Employees

20+ Countries

50 Years

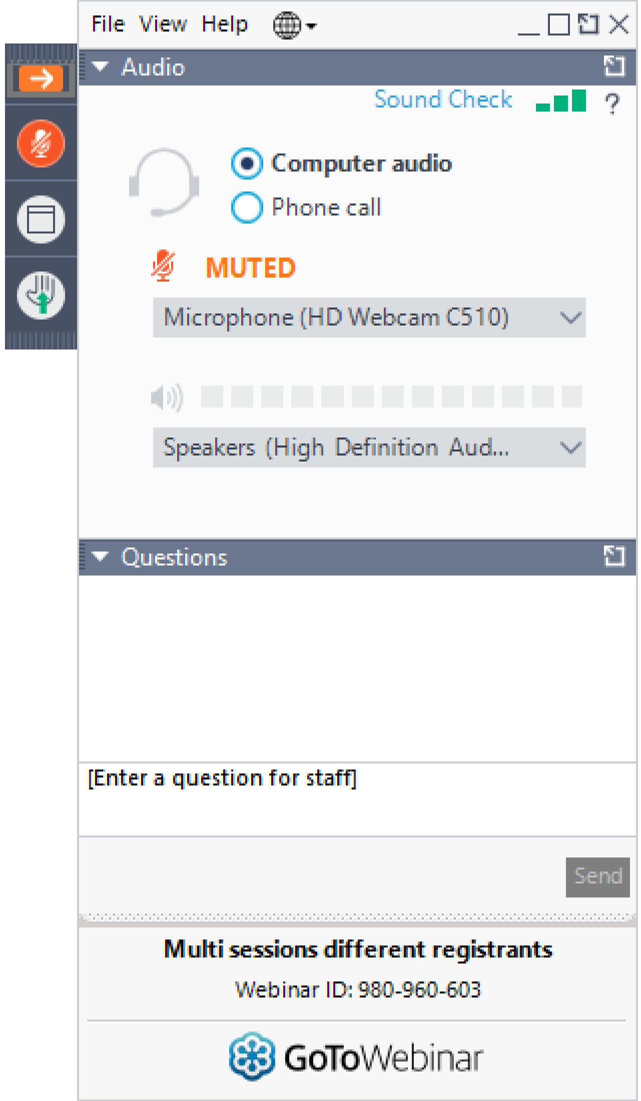


ABS Group is headquartered in Spring, TX, USA and is an independent subsidiary of ABS, one of the world's leading marine and offshore classification societies founded in 1862.

ABS Group

Questions

- Enter your question(s) in the GoToWebinar “Questions” section anytime throughout the presentation.
- A PDF copy of this webinar’s presentation is available in the “Handouts” section of the GoToWebinar panel.
- 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.



● Computer audio
○ Phone call

MUTED

Microphone (HD Webcam C510)

Speakers (High Definition Aud...

[Enter a question for staff]

Multi sessions different registrants

Webinar ID: 980-960-603

ABS Group

Objectives and Agenda

OBJECTIVES

- Understand current USCG requirements/recommendations and how to comply
- Learn how to utilize available grant funding opportunities for facilities

AGENDA

- Safety Moment
- Review: USCG NVIC 01-20
- Available Grant Funding for Cybersecurity at facilities
- Example project scopes
- Additional Resources
- Questions

Safety Moment – SSI

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

Ref: 49 CFR 1520

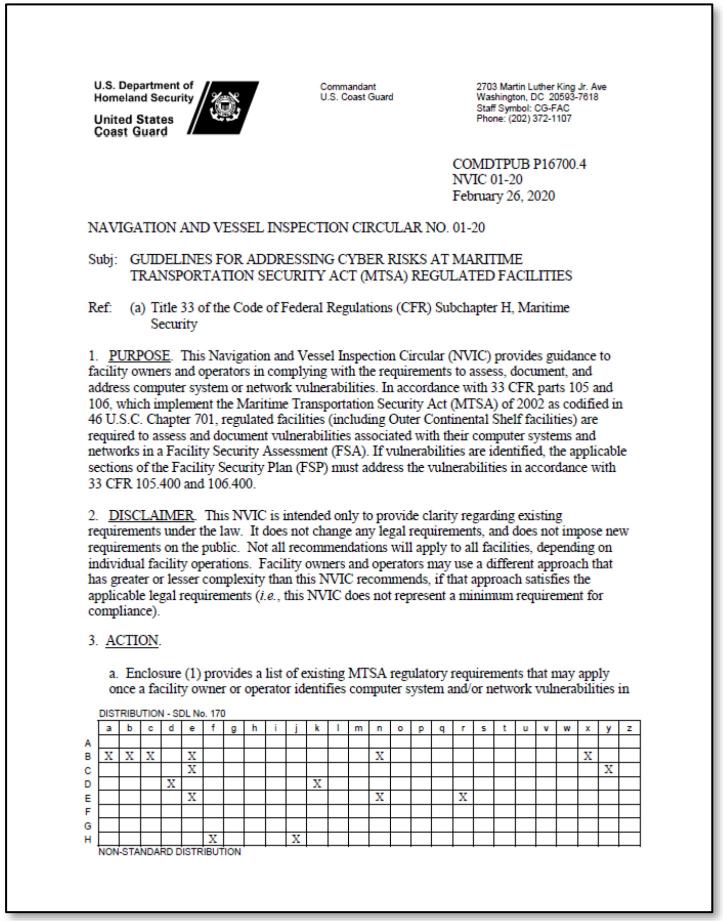
- Remember to always practice SSI when discussing facility security programs
- Hackers and criminals can easily obtain information about a facility network if openly discussed
- Treat cybersecurity the same as physical security - "Need to Know"

ABS GROUP
SAFETY CULTURE
ZERO LTI
2016 - 2017 - 2018 - 2019

AT WORK
AT HOME
ABS
TAKE 5
LOOK
BEGIN
THINK
CONTROL
RECOGNIZE

The Guidance: USCG NVIC 01-20

The 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 20593-7618
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 in

DISTRIBUTION - SDL 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																										
B	X	X	X		X									X										X		
C					X																				X	
D				X							X															
E					X									X				X								
F																										
G																										
H						X				X																

NON-STANDARD DISTRIBUTION

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

Facilities regulated under 33 CFR 105 and 106

33 CFR 105.305(c)(1)(v) & 106.305(c)(1)(v) require MTSA-regulated facilities to:

- Analyze vulnerabilities associated with radio and telecommunication equipment, including computer systems and networks

- Update or revise their FSAs and FSPs to address and mitigate any identified vulnerabilities.

- **33 CFR 105.220 & 106.225** describe how drills and exercises will test security vulnerabilities.

- **33 CFR 105.415(b) & 106.415(b)** describe audits and security plan amendments.

Implementation is due by September 30, 2021

(reference: ACN 040/20)

Connecting the Dots

LAW / REGULATION

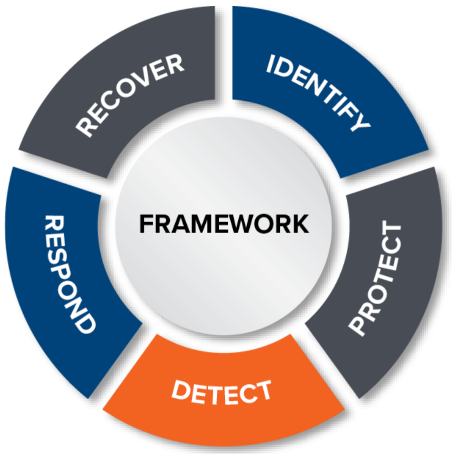
33 CFR 105/106

FACILITY SECURTY POLICY

NVIC 03-03

FACILITY CYBER POLICY

NVIC 01-20



NIST Cybersecurity Framework

Recommended Framework

NIST SP 800-82, Rev 2 – Guide to Industrial Control Systems (ICS) Security

USCG NVIC 01-20 Recommendations

1 Facility Security Assessments

2 Security Administration and Organization

3 Personnel Training

4 Drills and Exercises

5 Records and Documentation

6 Communications

7 Procedures for Interfacing with Vessels

8 Security Systems and Equipment Maintenance

9 Security Measures for Access Control

10 Security Measures for Restricted Areas

11 Security Measures for Handling Cargo

12 Security Measures for Delivery of Stores

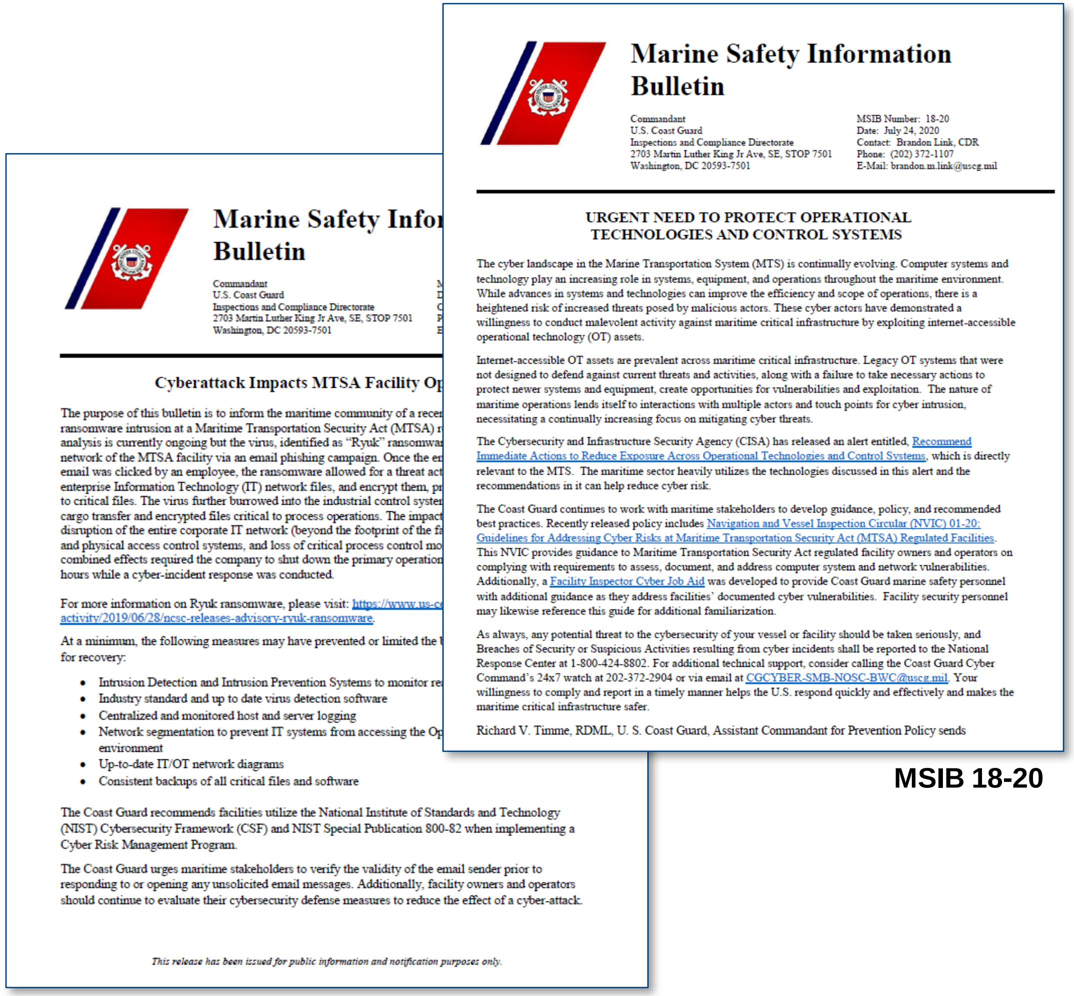
13 Security Measures for Monitoring

14 Facility Security Plan – Cyber Annex

15 Audits and Security Plan Amendments

ABS Group

Marine Safety Information Bulletins



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

Cyberattack Impacts MTSA Facility Op

The purpose of this bulletin is to inform the maritime community of a recen
ransomware intrusion at a Maritime Transportation Security Act (MTSA) r
analysis is currently ongoing but the virus, identified as "Ryuk" ransomwar
network of the MTSA facility via an email phishing campaign. Once the en
email was clicked by an employee, the ransomware allowed for a threat act
enterprise Information Technology (IT) network files, and encrypt them, pr
to critical files. The virus further burrowed into the industrial control systen
cargo transfer and encrypted files critical to process operations. The impact
disruption of the entire corporate IT network (beyond the footprint of the fa
and physical access control systems, and loss of critical process control mo
combined effects required the company to shut down the primary operation
hours while a cyber-incident response was conducted.

For more information on Ryuk ransomware, please visit: https://www.us-ce
activity/2019/06/28/ncsc-releases-advisory-ryuk-ransomware.

At a minimum, the following measures may have prevented or limited the t
for recovery:

- Intrusion Detection and Intrusion Prevention Systems to monitor re
- Industry standard and up to date virus detection software
- Centralized and monitored host and server logging
- Network segmentation to prevent IT systems from accessing the Op
  environment
- Up-to-date IT/OT network diagrams
- Consistent backups of all critical files and software

The Coast Guard recommends facilities utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82 when implementing a Cyber Risk Management Program.

The Coast Guard urges maritime stakeholders to verify the validity of the email sender prior to responding to or opening any unsolicited email messages. Additionally, facility owners and operators should continue to evaluate their cybersecurity defense measures to reduce the effect of a cyber-attack.

This release has been issued for public information and notification purposes only.

MSIB 10-19

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, equipment, and operations throughout the maritime environment. While advances in systems and technologies can improve the efficiency and scope of operations, there is a heightened risk of increased threats posed by malicious actors. These cyber actors have demonstrated a willingness to conduct malevolent activity against maritime critical infrastructure by exploiting internet-accessible operational technology (OT) assets.

Internet-accessible OT assets are prevalent across maritime critical infrastructure. Legacy OT systems that were not designed to defend against current threats and activities, along with a failure to take necessary actions to protect newer systems and equipment, create opportunities for vulnerabilities and exploitation. The nature of maritime operations lends itself to interactions with multiple actors and touch points for cyber intrusion, necessitating a continually increasing focus on mitigating cyber threats.

The Cybersecurity and Infrastructure Security Agency (CISA) has released an alert entitled, Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, which is directly relevant to the MTS. The maritime sector heavily utilizes the technologies discussed in this alert and the recommendations in it can help reduce cyber risk.

The Coast Guard continues to work with maritime stakeholders to develop guidance, policy, and recommended best practices. Recently released policy includes Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. This NVIC provides guidance to Maritime Transportation Security Act regulated facility owners and operators on complying with requirements to assess, document, and address computer system and network vulnerabilities. Additionally, a Facility Inspector Cyber Job Aid was developed to provide Coast Guard marine safety personnel with additional guidance as they address facilities' documented cyber vulnerabilities. Facility security personnel may likewise reference this guide for additional familiarization.

As always, any potential threat to the cybersecurity of your vessel or facility should be taken seriously, and Breaches of Security or Suspicious Activities resulting from cyber incidents shall be reported to the National Response Center at 1-800-424-8802. For additional technical support, consider calling the Coast Guard Cyber Command's 24x7 watch at 202-372-2904 or via email at CGCYBER-SMB-NOSC-BWC@uscg.mil. Your willingness to comply and report in a timely manner helps the U.S. respond quickly and effectively and makes the maritime critical infrastructure safer.

Richard V. Timme, RDML, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends

MSIB 18-20

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

MSIB's related to cybersecurity:

- **10-19:** Cyberattack Impacts MTSA Facility Operations
- **18-20:** Urgent Need to Protect Operational Technologies and Control Systems
- **25-20:** Urgent Notice: Active Exploitation of Popular Network Management Software SolarWinds
- **03-21:** Continued Awareness: Active Exploitation of SolarWinds Software

Beyond the Requirement…

- Preserve your facilities' reputation
- Emphasize **safety** in a cyber program
- The Sep. 30, 2021 deadline is fast approaching - meeting the requirements as soon as possible will contribute to compliance status as well as overall cyber security posture
- In NVIC 01-20, the Coast Guard makes it very clear that performing cybersecurity assessments and addressing cybersecurity in FSP is a requirement.
- **Implementing Cyber Risk Management will put you in a better position to be more competitive.**

ABS Group

Grant Funding Opportunities

Port Security Grant Program (PSGP)

- Administered by FEMA
- Description:
  “This grant provides funding to state, local and private-sector partners to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency.”
- Key Dates:
  - Application due around April/May
  - Announcement of funding around July/August
- Application Effort – Four (4) weeks
- 25-50% Grantee Cost Share

https://www.fema.gov/grants/preparedness/port-security

Port Infrastructure Development Program (PIDG)

U.S. Department of Transportation
Maritime Administration

- Administered by Maritime Administration (MARAD)
- Description:
  "… grants to improve the safety, efficiency, or reliability of the movement of goods into, out of, around, or within coastal seaports, inland river ports, or Great Lakes ports…"
- Key Dates – 2021:
  - Application due July 30th, 2021
  - Announcement TBD
- Application Effort – Two (2) to four (4) weeks
- 20% Grantee Cost Share

https://www.maritime.dot.gov/PIDPgrants

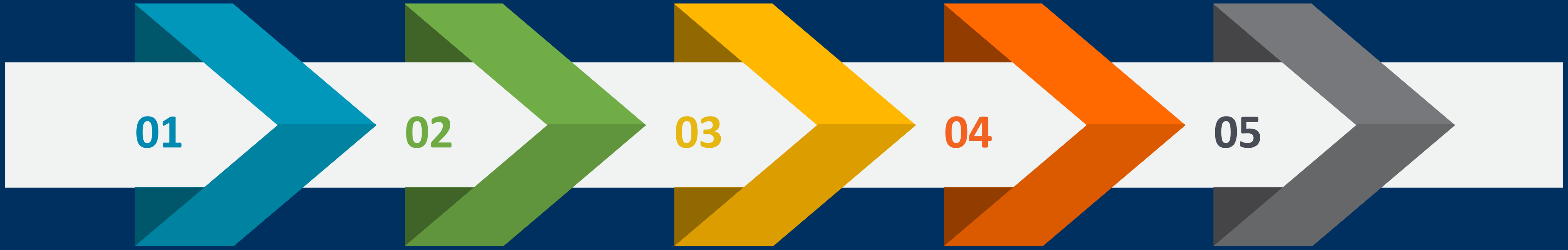
ABS Group

How to Apply Grant Funding to Cybersecurity Efforts

Cyber Facility Security Assessment

OBJECTIVE: Conduct a facility cybersecurity assessment to discover gaps and vulnerabilities in current cybersecurity program

SCOPE:



01 Project introduction and support from leadership

02 Plan facility assessment based on a recognized standard like NIST CSF

03 Evaluate existing cybersecurity documents and conduct interviews of key personnel

04 Compile assessment report

05 Roadmap to address identified gaps

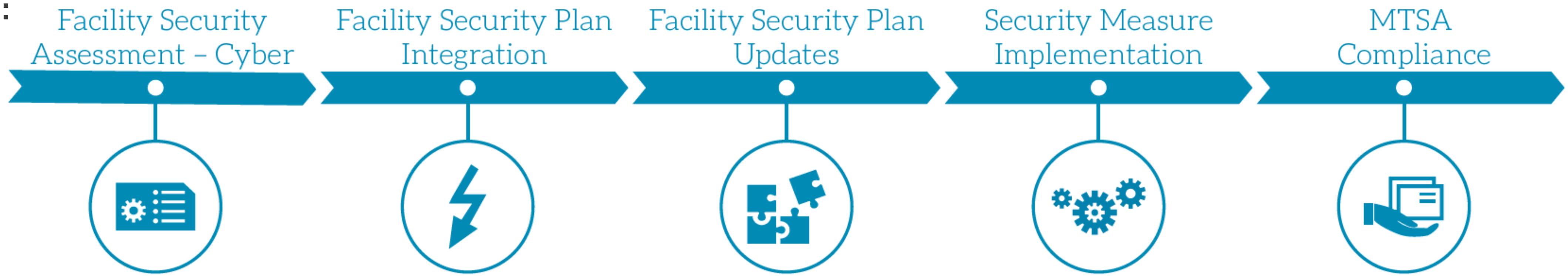
KEY CONSIDERATIONS:

- Assessment should identify the security weaknesses, technical protections and vulnerabilities discovered on a facility network for both Operational Technology (OT) and Information Technology (IT) if tied into OT devices
- Important for the assessor to combine physical security standards
- Recommended stakeholder participation: FSO/AFSO, IT, OT, Operations Staff, Management, HSSE/SHE

Facility Security Plan Update – Cyber Annex

OBJECTIVE: Cyber risk management update or integration into Facility Security Plan (FSP).

SCOPE:



Facility Security Assessment – Cyber

Facility Security Plan Integration

Facility Security Plan Updates

Security Measure Implementation

MTSA Compliance

KEY CONSIDERATIONS:

- Consider creating a cybersecurity Annex for your existing FSP vs performing changes to the FSP
  - Amendment required for each change

- The cybersecurity Annex or Plan Updates should include:
  - List of Critical OT
  - Cyber vulnerabilities identified in the FSA
  - Incident response plan
  - Roles and responsibilities

Cyber Incident Training

OBJECTIVE: Ensure proper implementation of Cyber Incident Response Plan

TASKS

1. Determine training method (Instructor-Led, eLearning, etc.)
2. Look at existing resources
3. Establish objectives and outline key information from Cybersecurity Plan
4. Get feedback and edit as needed before rollout

KEY CONSIDERATIONS

- After completing training, personnel should be able to answer the following:
  - What processes are executed once an incident is identified?
  - Who is responsible, accountable, consulted and informed for each step of the processes?
  - What roles do legal, IT, OT, law enforcement, marketing, HR and executives play?
  - What resources are available and when should you use them?
- Consider including knowledge checks to test effectiveness

Cyber Incident Drills and Exercises

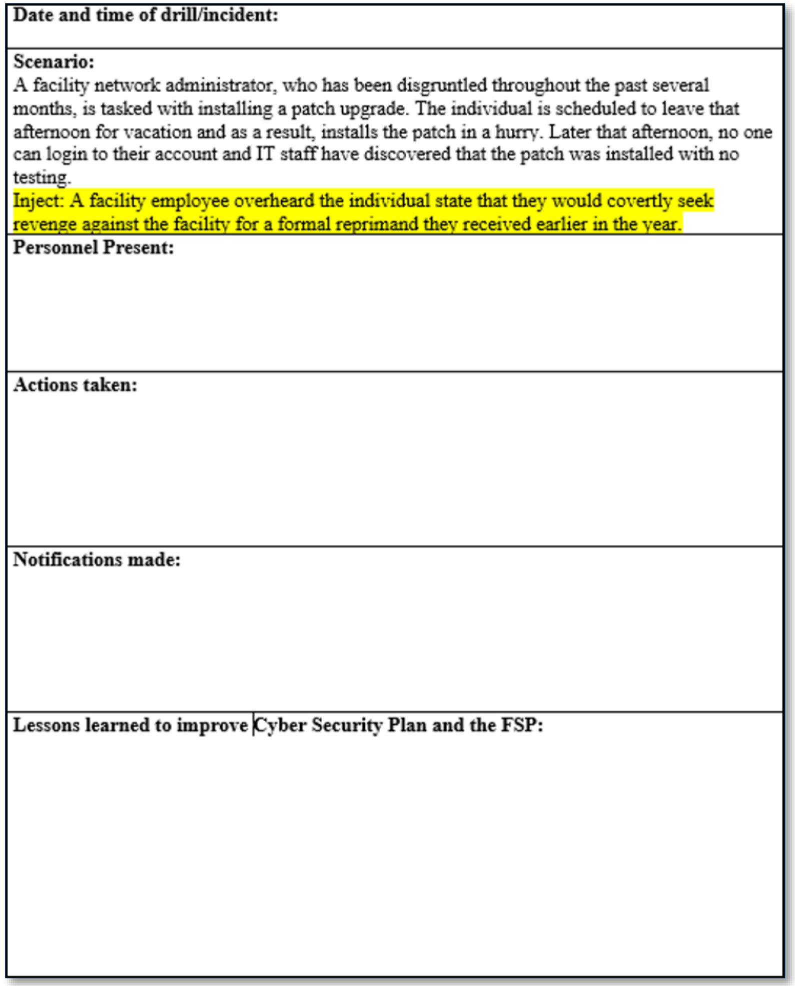
OBJECTIVE: Test newly implemented facility cybersecurity measures and incident response plan.

SCOPE:

1. Use third-party or appoint a designated internal lead to coordinate and execute the drill/exercise (drill vs. exercise – one aspect vs whole plan)
2. Appointed lead develops scenario (can be tabletop exercise or series of individually conducted interviews)
3. Execute scenario as tabletop exercise or series of individually conducted interviews
4. Review lessons learned

KEY CONSIDERATIONS:

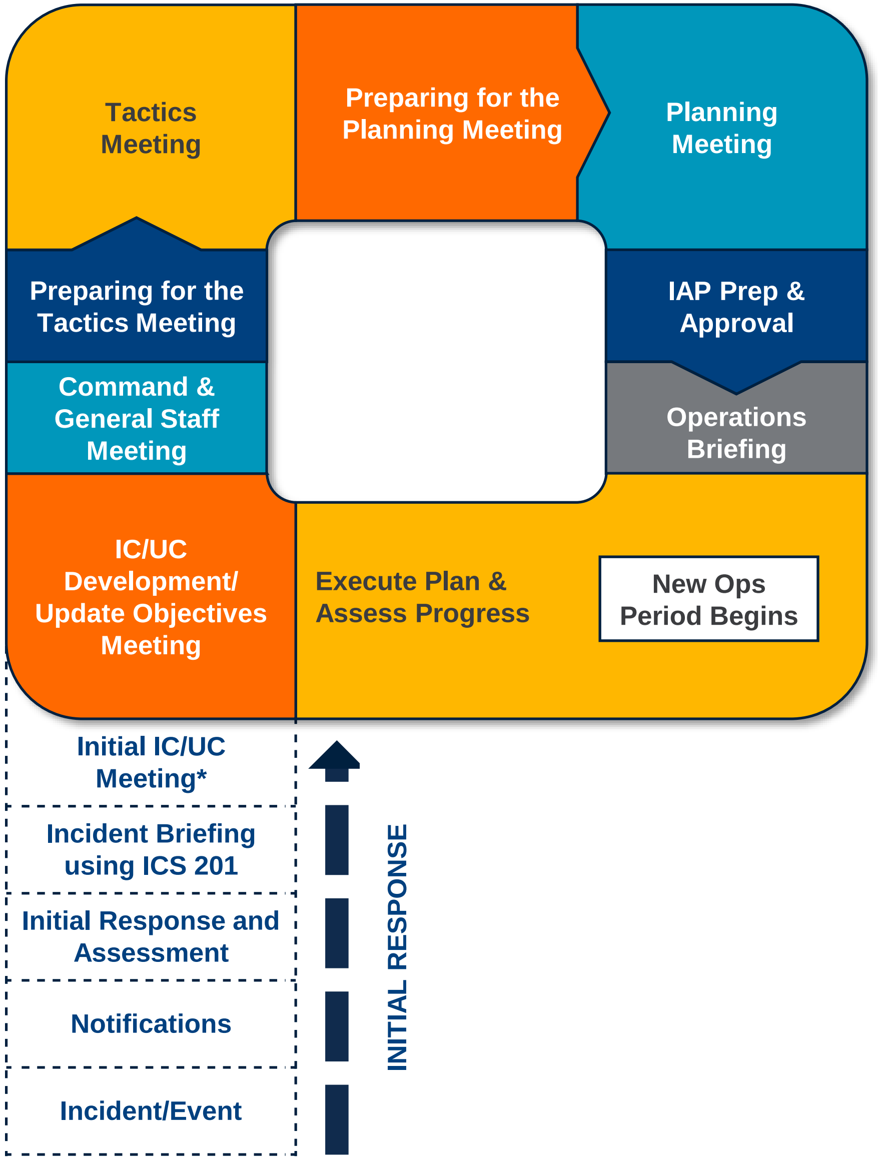
- Exercise required annually (not to exceed 18 months)
- Drills should:
  - Enhance response capabilities
  - Bridge the gap between FSOs and cyber staff
  - Raises awareness/build culture
  - Identify incident response shortfalls
  - Combine physical-cyber scenarios
- Use the Incident Command System (ICS) during a cyber incident



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

- Include as part of drills and exercises
- Be creative: 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)
- Avoid "battlefield introductions"- exercise regularly



Tactics Meeting

Preparing for the Planning Meeting

Planning Meeting

Preparing for the Tactics Meeting

IAP Prep & Approval

Command & General Staff Meeting

Operations Briefing

IC/UC Development/ Update Objectives Meeting

Execute Plan & Assess Progress

New Ops Period Begins

Initial IC/UC Meeting*

Incident Briefing using ICS 201

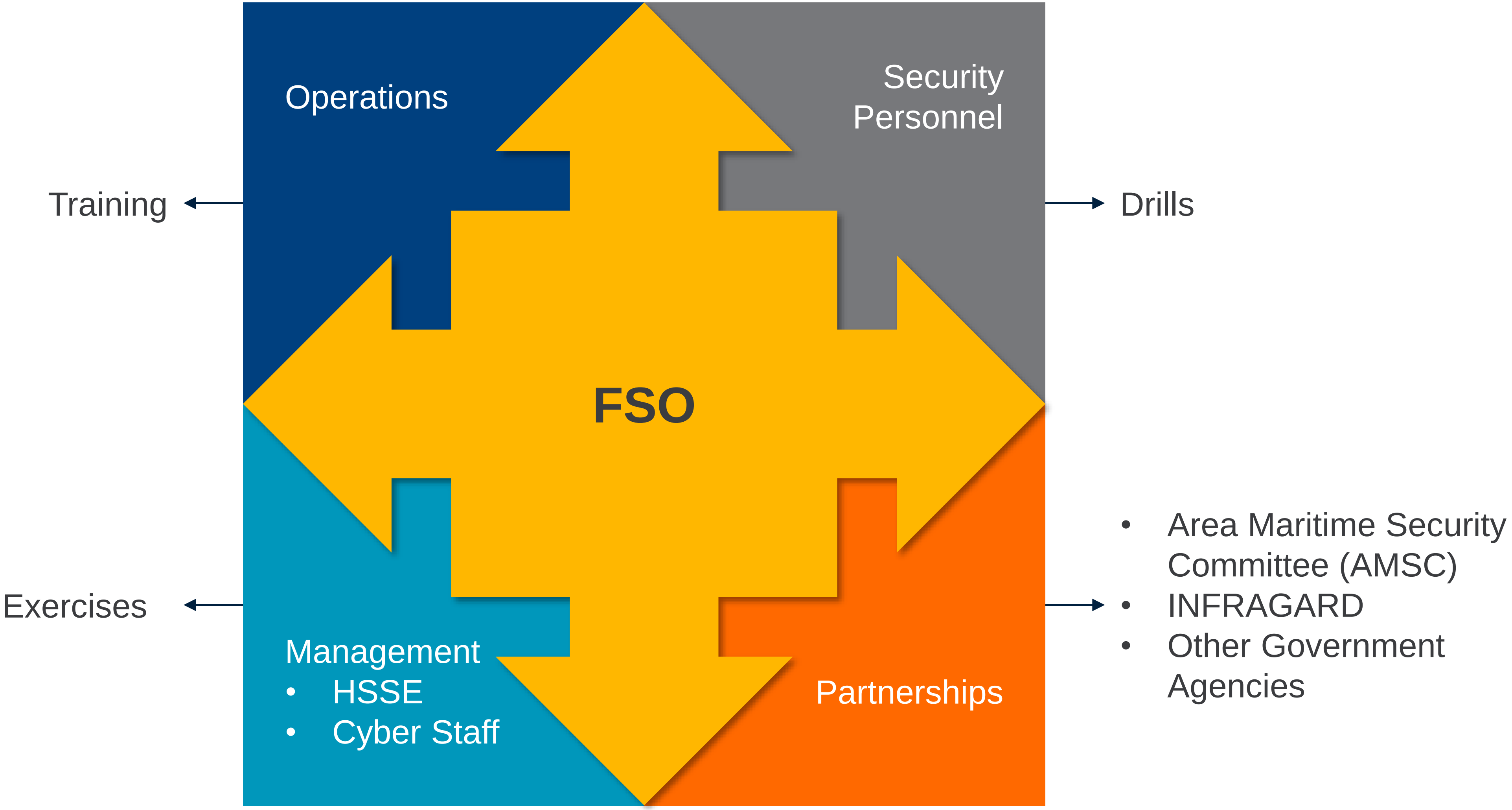
Initial Response and Assessment

Notifications

Incident/Event

INITIAL RESPONSE

Facility Security Officer Cyber Square



- Area Maritime Security Committee (AMSC)
- INFRAGARD
- Other Government Agencies

ABS Group

OT Network Visibility Pilot

OBJECTIVE: Provide depth and breadth of visibility across the OT networks.

SCOPE:

1. Select technologies to aid in the detection of threats, tracking of assets and discovery of vulnerabilities
    - Technologies should monitor network traffic on the installed networks and collect threat, asset and vulnerability information locally at the facility
2. Scope technology placement and set objectives (i.e. asset inventory, vulnerability analysis, etc..)
3. Set data collection period (recommended 30-60 days)
4. Perform analysis and processing if needed

Key Considerations:

- Set both short-term and long-term objectives
- Consider how this data can be used to eventually set up a continuous monitoring solution
- Identify technologies which are intended specifically for the operational environment

Additional Resources

Cybersecurity 101: Lessons Learned from the Colonial Pipeline Cyber Attack [On-Demand Webinar]

OT Cybersecurity: How to Evolve Faster Than Cyber Criminals [On-Demand Webinar]

Understanding Cybersecurity Through the Lens of USCG NVIC 01-20 [On-Demand Webinar]

A Primer on Cybersecurity for MTSA-Regulated Facilities

Subscribe to Our Podcast:

EPISODE 13
The Casualties of Cyber War:
Exploring the Colonial Pipeline Shutdown

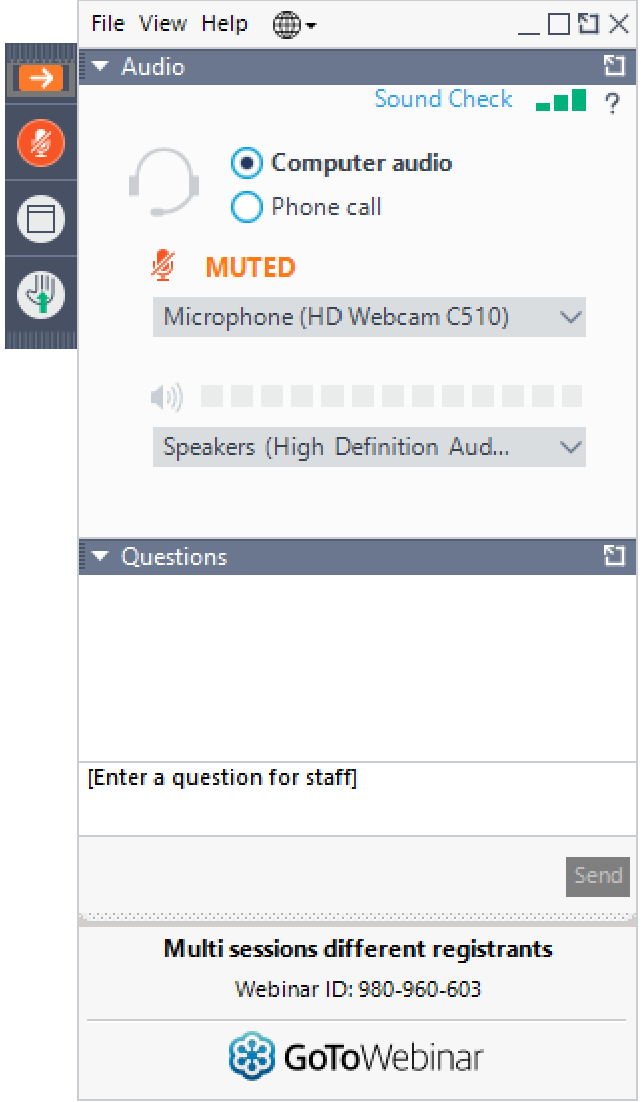
EPISODE 3
Emergency Response and Facility Security Perspectives

-- Search Risk Matters X.0 on Spotify, Apple or Google Podcasts --

ABS Group

Questions

- Enter your question(s) in the GoToWebinar “Questions” section at this time.
- A PDF copy of this webinar’s presentation is available in the “Handouts” section of the GoToWebinar panel.
- 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.



● Computer audio
○ Phone call

MUTED

Microphone (HD Webcam C510)

Speakers (High Definition Aud...

[Enter a question for staff]

Multi sessions different registrants

Webinar ID: 980-960-603

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

Ref: 49 CFR 1520

ABS Group

ABS Group

Thank You

www.abs-group.com

in linkedin.com/company/absgroup

@_absgroup

Marcia Lee
Business Development Manager, Cybersecurity
Marlee@absconsulting.com
+ 1 281.387.3835

Brian Shajari
Senior Cybersecurity Assessor
BShajari@absconsulting.com
+1 703.351.3700

ABS Group