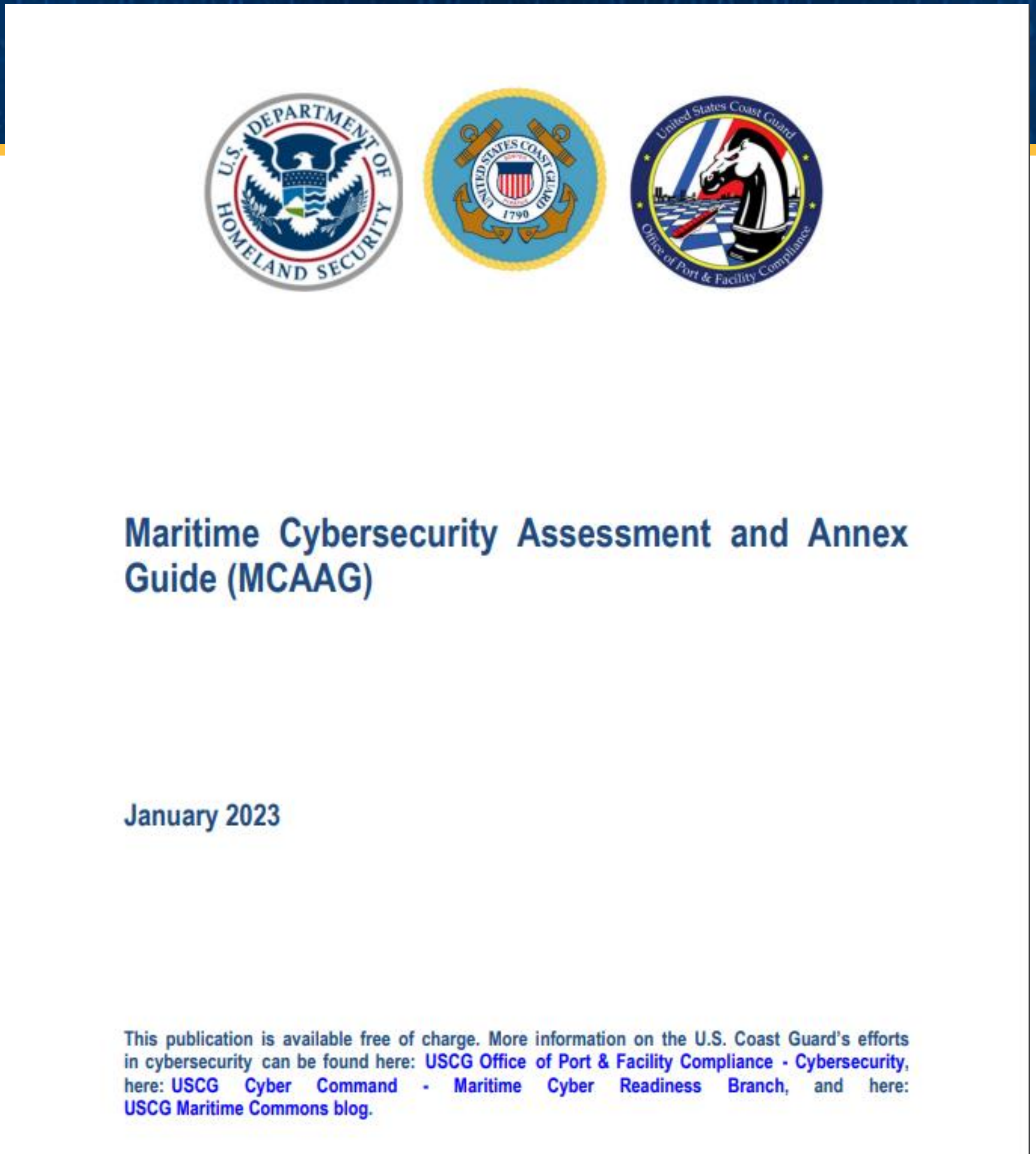
Maritime Cybersecurity Assessment & Annex Guide (MCAAG)

Office of Port & Facility Compliance

A Nation Safeguarded by a Cyber Enabled Coast Guard

Overview

- **Goals & Challenges of Cyber Annex Guide**
- **Primary Features of Cyber Annex Guide**



Maritime Cybersecurity Assessment and Annex Guide (MCAAG)

January 2023

This publication is available free of charge. More information on the U.S. Coast Guard's efforts in cybersecurity can be found here: USCG Office of Port & Facility Compliance - Cybersecurity, here: USCG Cyber Command - Maritime Cyber Readiness Branch, and here: USCG Maritime Commons blog.

Goals & Challenges

Cyber Annex Is a Form of Assessment → Risk Management

- **Risk Management requires Assessments inputs**
  - Operational status
  - Threats & Vulnerabilities
  - Consequences
- **Current MCRAM and Cyber Annex Guide constrained by current tempo, availability, accuracy, consistency of USCG assessment data for MTS**
  - Sources: MCRB engagements, current FSA/FSPs, open source (threat info)
- **More standardized & detailed Cyber Annexes (assessments) would incrementally improve USCG situational awareness (SA) and resulting risk management**

Guide Must Work for Low Cyber Maturity MTS Facilities

- **Like most sectors, the MTS can be broken into 3 groups in terms of cybersecurity maturity**
  - High: Well established policy and governance; APT defenders
  - Medium: Meets or exceeds basic hygiene; Commercial grade defenses
  - Low: Fails to meet basic hygiene; Inadequate defenses
- **Cyber Annex**
  - Must-have: helps low maturity facilities
  - Nice-to-have: relevant to high facilities
- **MTS Maturation Issues**
  - IT/OT fusion: Understood by medium and high
  - IT/OT/BCS fusion: Understood by high only

Guide Must Balance USCG Physical Security Mandate Against "All Cybersecurity" Reality

- **USCG authority is for physical security and related cyber**
- **Physical security depends on <u>ALL</u> cybersecurity in a facility**
- **Guide must:**
  - Relate to direct cyber security implications of NVIC 01-20 and associated CFRs regarding physical security dependencies on cybersecurity
  - Provide sufficient facility-wide cybersecurity to be credible
  - Avoid over-reach into all cybersecurity (thus causing industry pushback)

Primary Features

Cybersecurity Officer (CySO)

- **Partner to FSO with adequate knowledge of information technology (IT), Operational Technology (OT), and Building Control and Security (BCS) infrastructure and cybersecurity**
  - Could be a group or the FSO themself
- **Section 2 & 3 provide FSO-oriented guidance**
  - Notional architecture: IT, OT, BCS
  - Associated cyber attacks
  - Cyber Annex development process
  - Just enough information to facilitate collaboration with CySO
- **Appendices provide more detailed CySO-oriented guidance**
  - Annex Template, CSF-based Cybersecurity Baseline, Implementation Guidance

Cyber Annex Definition of "Cybersecurity Vulnerability"

- **Concept of "Vulnerability" is flexible and must be tailored to specific situation**
- **For FSP & Cyber Annex, a <u>cybersecurity vulnerability</u> is:**
  - Defined at level of CSF subcategories
    - MTS not mature enough to sustain assessment at a more granular level
  - A deficiency in basic cybersecurity hygiene
    - MTS not mature enough to respond to more aggressive recommendations
    - Unclear if USCG authority justifies more
  - Or a deficiency in protection of system directly related to FSA physical vulnerabilities
    - Clearly within USCG authority

CSF-based Cybersecurity Baseline

- **CSF subcategory selection defined at three levels:**
  - Low: Baseline
  - Medium: Additional Recommendations
  - High: Entire CSF
- **Selections based on**
  - Relevant industry standards & guidance including:
    - NVIC 01-20
    - MCRB guidance & Industry-standard cybersecurity hygiene practices
    - MTS-related CSF Profiles
    - Review by NMSAC
  - USCG Mission Priorities
    - Safety
    - Continuity of Operations

Process Flow

1. Identify a person or committee to act as the CySO in support of the FSO
2. Identify all cyber-enabled systems and networks related to the physical security vulnerabilities in the FSA
3. Agree on a facility definition of “cybersecurity vulnerability” in the context of the FSA
4. Gather information necessary to identify cybersecurity vulnerabilities and finalize the list to be addressed in the Cyber Annex
5. Determine the remediation plan for each vulnerability expressed in terms of cybersecurity protections appropriate for the facility
6. Use the provided template to document the physical vulnerabilities in the FSP, the cybersecurity vulnerabilities, any relationships between them, and the protections within the facility’s cybersecurity plan

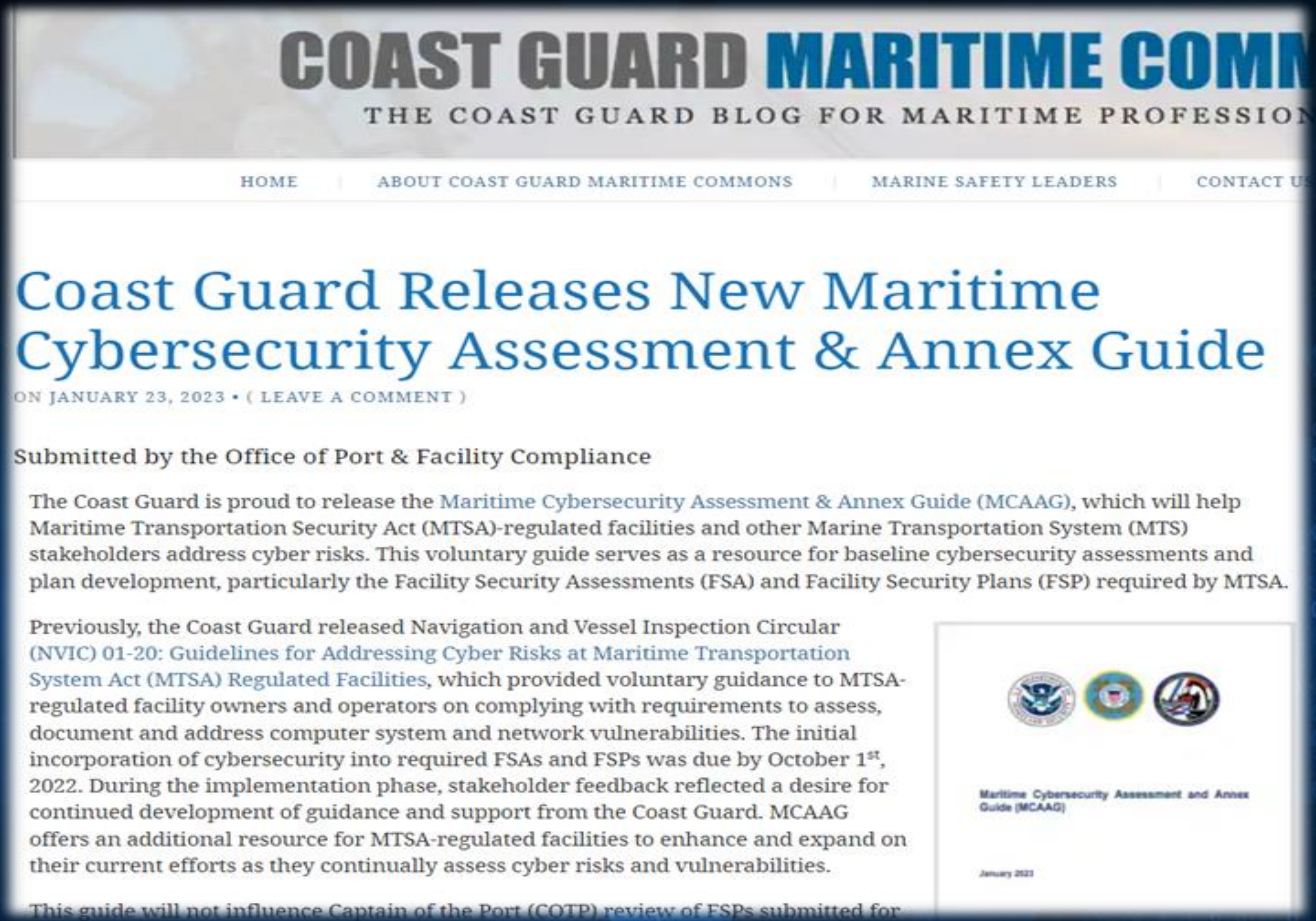
Cyber Annex Template

1. **List the physical security vulnerabilities from the FSA and FSP with identifiers and organized according to the categories specified in 33 CFR 105.405 (a).**
   - Alternatively, list the FSA vulnerabilities with identifiers and provide a traceability matrix between them and the categories specified in 33 CFR 105.405(a).
2. **List the cybersecurity vulnerabilities to be addressed in the Cyber Annex with identifiers.**
   - Provide a traceability matrix between the cybersecurity vulnerabilities and their associated physical security vulnerabilities.
3. **List the cybersecurity protections that will collectively address the identified cybersecurity vulnerabilities.**
   - Provide a traceability matrix between the cybersecurity protections and the cybersecurity vulnerabilities they remediate.
   - Provide a traceability matrix between the cybersecurity protections and NIST CSF subcategories.

Additional Guidance (Example – Based on MCRB Inputs)

Records and Documentation

- **Threat Summary**
  - Inadequately trained users, operators, and administrators may be susceptible to threat actors (e.g., spear phishing). Attackers may access systems to compromise the confidentiality, integrity, or availability of electronic records. They may access or exfiltrate sensitive information (e.g., client, cargo, or proprietary data) risking facility or MTS operations.
  - Ransomware attacks can cause operational delays until the facility can restore systems and data
- **CSF Baseline Guidance**
  - Apply PR.AT baseline controls (PR.AT-1 through PR.AT-5) to ensure personnel can identify a potential campaign/attack and know how to respond accordingly
  - Implement ID.AM-1, ID.AM-2 to ensure the facility maintains an inventory of systems and software that hold electronic records and need to be protected
  - Implementation of PR.IP-4, PR.IP-6 ensures the facility has adequate data retention policy and backups of electronic records
  - Implementation of PR.DS-1, PR.DS-5 protects the integrity and confidentiality of the electronic records
  - Implement PR.AC baseline controls (PR.AC 1 through PR.AC-7) to prevent unauthorized modification of records
- **Sample Additional Cybersecurity Protections**
  - Ensure integration of records system into related processes
    - Maintain an inventory of electronic record systems
  - Electronic records systems should be protected by application of complete cybersecurity program (CSF)



COAST GUARD MARITIME COMM

THE COAST GUARD BLOG FOR MARITIME PROFESSION

Coast Guard Releases New Maritime Cybersecurity Assessment & Annex Guide

ON JANUARY 23, 2023 • (LEAVE A COMMENT)

Submitted by the Office of Port & Facility Compliance

The Coast Guard is proud to release the Maritime Cybersecurity Assessment & Annex Guide (MCAAG), which will help Maritime Transportation Security Act (MTSA)-regulated facilities and other Marine Transportation System (MTS) stakeholders address cyber risks. This voluntary guide serves as a resource for baseline cybersecurity assessments and plan development, particularly the Facility Security Assessments (FSA) and Facility Security Plans (FSP) required by MTSA.

Previously, the Coast Guard released Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation System Act (MTSA) Regulated Facilities, which provided voluntary guidance to MTSA-regulated facility owners and operators on complying with requirements to assess, document and address computer system and network vulnerabilities. The initial incorporation of cybersecurity into required FSAs and FSPs was due by October 1st, 2022. During the implementation phase, stakeholder feedback reflected a desire for continued development of guidance and support from the Coast Guard. MCAAG offers an additional resource for MTSA-regulated facilities to enhance and expand on their current efforts as they continually assess cyber risks and vulnerabilities.

Maritime Cybersecurity Assessment and Annex Guide (MCAAG)

January 2023

This guide will not influence Captain of the Port (COTP) review of FSPs submitted for

Office of Port and Facility Compliance (CG-FAC) Website

Maritime Cyber Readiness Branch (MCRB) Website - *maritimecyber@uscg.mil*

A Nation Safeguarded by a Cyber Enabled Coast Guard