# Supporting Statement
# for
# Cybersecurity Plans

(as modified by USCG-2022-0802; RIN 1625-AC77)

OMB No.: 1625-0132
COLLECTION INSTRUMENTS: Instruction

## A. Justification

1. Circumstances that make collection of information necessary.

Under the Maritime Transportation Security Act of 2002 (MTSA),[1] Congress provided a framework for the Coast Guard and maritime industry to identify, assess, and prevent security incidents in the marine transportation system (MTS). In 2013, 2015, and 2021, Congress reaffirmed that framework through amendments to MTSA. It tasked the Coast Guard, through the Secretary of the Department of Homeland Security (DHS), with ensuring that Facility Security Plans (FSPs), Outer Continental Shelf (OCS) FSPs, and Vessel Security Plans (VSPs) include provisions to prevent and respond to transportation security incidents (TSI), including cybersecurity incidents.[2]

The purpose of the cybersecurity regulations is to safeguard the MTS against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements to 33 Code of Federal Regulations (CFR) part 101. The regulations apply to the owners and operators of U.S.-flagged vessels subject to 33 CFR part 104 (Maritime Security: Vessels), facilities subject to 33 CFR part 105 (Maritime Security: Facilities), and OCS facilities subject to 33 CFR part 106 (Marine Security: Outer Continental Shelf (OCS) Facilities). The requirements include account security measures, device security measures, data security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security.

The statutory authority for the requirements are 43 U.S. Code (U.S.C.) 1333(d); 46 U.S.C. 3306, 3703, 70102 through 70104, and 70124. This authority is delegated by the Secretary to the Coast Guard via the Department of Homeland Security (DHS) Delegation No. 00170(II), Revision No. 01.3, (90), (92)(b), and (97)(a) through (c).

2. Purpose of the information collection.

The primary need for information is to determine if stakeholders are in compliance with cybersecurity standards. The required collection of information is also important for stakeholders to determine and design appropriate security measures for the safety of their assets. The information can also help determine, in the case of TSI, whether failure to meet these regulations contributed to the TSI.

3. Consideration of the use of improved information technology.

Security plans, assessments, amendments and audits, and related material, can be submitted electronically via https://homeport.uscg.mil/ or as an attachment to an e-mail to securityplaninfo@uscg.mil. We estimate that 95% of the reporting and recordkeeping requirements are done electronically.

Regarding Usability Testing, this ICR—

- Public-facing instructions were tested by the staff of the CG Office of Standards Evaluation and Development (CG-REG) to ensure the use of plain language. Usability testing participants

[1] Pub. L. 107-295, 116 Stat. 2064, November 25, 2002.
[2] 46 U.S.C. 70103(c)(3)(C)(v).

reported that they had no difficulty understanding the instructions. As a result, the USCG did not make any changes to the collection.
- Is not related to a public benefit program as detailed in OMB M-22-10 (titled “Improving Access to Public Benefits Programs Through the Paperwork Reduction Act” dated April 13, 2022).
- Does not require the use of a form or specify a reporting format/method.
- Is required by international treaty, statute, and/or regulation as notes in section 1 of the Supporting Statement.

4. Efforts to identify duplication.

The Coast Guard monitors State and local regulatory activity in this field. To date, no other equivalent State or local programs have been identified that require similar information.

5. Methods to minimize the burden to small entities if involved.

Because of the nature of the information collection requirements, the level of effort to prepare a VRP or FRP is estimated to vary directly with the size and complexity of the entity. As a result, smaller entities should incur a lesser burden than larger entities.

6. Consequences to the Federal program if collection were conducted less frequently.

The Coast Guard has determined that requiring entities to review and update their plans less frequently than once a year (after initial submission) would undermine the intent of MTSA, which is to ensure that all entities have an up-to-date plan at all times, because plans are used to reduce the risk of a TSI.

7. Special collection circumstances.

This information collection is conducted in manner consistent with the guidelines in 5 CFR 1320.5(d)(2).

8. Consultation.

The Coast Guard published on February 22, 2024, a Notice of Proposed Rulemaking (NPRM) entitled “Cybersecurity in the Marine Transportation System” (Cyber) [USCG-2022-0802; RIN 1625-AC77; 89 FR 13404]. The rulemaking proposed to—
- update its maritime security regulations by adding regulations specifically focused on establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to the Maritime Transportation Security Act of 2002 regulations. This proposed rule would help to address current and emerging cybersecurity threats in the marine transportation system.

The NPRM comment period (with a 30-day extension [89 FR 24751]) closed on May 22, 2024. The Coast Guard received no collection of information-related comments to the NPRM. On January 17, 2025, the Cyber Final Rule was published [90 FR 6298].

9. Explain any decision to provide payment or gift to respondents.

There is no offer of monetary or material value for this information collection.

10. Assurance of confidentiality provided to respondents.

The information will be kept private or anonymous to the extent allowable by law. Confidentiality/security of information contained in vessel, facility, and OCS facility security assessments and plans is of vital importance. MTSA (46 U.S.C. section 70101(d)) require documents related to security, especially security assessments and plans, to be kept in a manner that is protected from unauthorized access or disclosure. Understanding the imperative need to safeguard maritime security material to ensure its

dissemination does not make the vessel or facility vulnerable to a TSI, the Coast Guard has included provisions in these regulations noting that this type of material is to be designated as sensitive security information (SSI) in accordance with 49 CFR part 1520. Information designated as SSI is generally exempt under FOIA, and the Coast Guard believes that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation.

This information collection request is not privacy sensitive therefore, it does not require coverage from a Privacy Impact Assessment (PIA) or a System of Records Notice (SORN).

11. Additional justification for any questions of a sensitive nature.

There are no questions of sensitive language.

12. Estimates of reporting and recordkeeping hour and cost burdens of the collection of information.

- The estimated annual number of respondents is 5,793.
- The estimated annual number of responses is 5,793.
- The estimated annual hour burden is 268,900 hours.
- The estimated annual cost burden is $24,201,000.

The burden to respondents is in Appendix A. The collections of information for the cybersecurity regulations are primarily contained in the vessel/facility security assessment and plans. The resulting burden hours are therefore for planning, developing and writing these security assessments and plans. We expect that a Security Specialist conducts the assessments and develop the plans. Collections of information under each part are described below. For the wage rate, we used the Bureau of Labor Statistics (BLS) wage rate for Information Security Analysts (15-1212) [May 2023, mean hourly wage, loaded 50%, and rounded].[3]

A. For vessels, we assume each company will prepare the core cybersecurity documents, and there will be an incremental cost for each vessel included in the assessment or plan. We estimate that it takes 40 hours for the initial cybersecurity assessment and plan development. Additionally, we estimate the annual review and 5-year periodic review/resubmission (per response) are 8 and 12 hours respectively.

Each assessment and plan is tailored to meet the different needs of each vessel, so the number of annual responses is equal to the total number of vessels affected by the regulation. Vessel population is derived from the Coast Guard's MISLE[4] database. See Appendix A for the calculation of burden.

B. For facilities (shoreside and OCS), we assume each facility will prepare the cybersecurity documents. We estimate that it takes 50 hours for the initial cybersecurity assessment and plan development. Additionally, we estimate the annual review and 5-year periodic review/resubmission (per response) are 10 and 15 hours respectively.

Each assessment and plan is tailored to meet the different needs of each facility, so the number of annual responses is equal to the total number of facilities affected by the regulation. Facility population is derived from the Coast Guard's MISLE database. See Appendix A for the calculation of burden.

13. Estimates of annualized capital and start-up costs.

No capital start-up cost associated with this collection.

14. Estimates of annualized Federal Government costs.

[3] https://www.bls.gov/oes/2023/may/oes151212.htm

[4] Marine Information for Safety and Law Enforcement

The estimated annual Federal Government cost is $1.99 million (see Appendix B). The cost includes Federal personnel costs and contract costs. Review of cybersecurity vessel and facility plans—new, annual and 5-year resubmission—are conducted by the Coast Guard at separate locations. Vessel plans are reviewed at the U.S. Coast Guard Marine Safety Center.[5] Facility plans are reviewed by the local Coast Guard units (e.g., Sector Offices).[6] We estimate that facility plan reviews are done by a Coast Guard Lieutenant (LT, O-3). The wage rate shown is in accordance with the current edition of COMDTINST 7310.1(series) for "In-Government" personnel.

15. Explain the reasons for the change in burden.

This is a new collection.

16. Plans for tabulation, statistical analysis and publication.

This information collection will not be published for statistical purposes.

17. Approval to not display expiration date.

The Coast Guard will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement.

The Coast Guard does not request an exception to the certification of this information collection.

**B. Collection of Information Employing Statistical Methods**

This section does not apply because the collection does not employ statistical methods.

[5] The reviews are done by a contract staff.

[6] Local Coast Guard units manage facility security plan reviews. The reviews are done by Federal personnel. Cost calculated as follows—# CG Sector Offices x LT hourly wage rate x .5 LT Annual-staff-time (FTE)/unit (i.e., 1,000 hours) (rounded).