Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

FPRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit https://www.dhs.gov/privacy-office-contacts. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Financial Responsibility-Vessels; Superseded Funds		
Component or Office:	U.S. Coast Guard (USCG)	**Office or Program:**	National Pollution Funds Center
FISMA Name (if applicable):	N/A	**FISMA Number (if applicable):**	N/A
Type of Project or Program:	Rule	Project or program status:	Update
Date first developed:	N/A	**Pilot launch date:**	N/A
Date of last PTA update	N/A	**Pilot end date:**	N/A
ATO Status (if applicable):[1]	Choose an item.	**Expected ATO/ATP/OA date (if applicable):**	N/A

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	Benjamin White		
Office:	National Pollution Funds Center	**Title:**	Project Manager/Economist
Phone:	(202) 795-6066	**Email:**	Benjamin.H.White@uscg.mil

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**N/A**		
Phone:	**N/A**	**Email:**	N/A

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Authority%20to%20Proceed%20Memo%20Phase%20II.pdf.

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
The Coast Guard is amending its rule on vessel financial responsibility to include tank vessels greater than 100 gross tons, clarify and strengthen the rule's reporting requirements, conform to current practice, and to remove two superseded regulations. This rulemaking will ensure the Coast Guard has current information when there are significant changes in a vessel's operation, ownership, or evidence of financial responsibility, and reflect current best practices in the Coast Guard's management of the Certificate of Financial Responsibility program. This rulemaking will also promote the Coast Guard's missions of maritime stewardship, maritime security and maritime safety.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☒ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[2] ☐ Members of the public ☐ U.S. Persons (U.S citizens or lawful permanent residents) ☐ Non-U.S. Persons ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
2(a) Is information meant to be collected from or about sensitive/protected populations?	☒ No

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

	☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[3] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

3. What specific information about individuals is collected, maintained, used, or disseminated?

None

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[4] If applicable, check all that apply.

☐ Social Security number	☐ Social Media Handle/ID
☐ Alien Number (A-Number)	☐ Biometric identifiers *(e.g., FIN, EID)*
☐ Tax Identification Number	☐ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.*
☐ Visa Number	
☐ Passport Number	☐ Other. *Please list: Click here to enter text.*
☐ Bank Account, Credit Card, or other financial account number	
☐ Driver's License/State ID Number	

3(b) Please provide the specific legal basis for the collection of SSN:	N/A

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

[3] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf.

[4] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[5] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

Click here to enter text.
3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[6] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*
N/A

4. How does the Project, Program, or System retrieve information?	☐ By a unique identifier.[7] Please list all unique identifiers used: *Click here to enter text.* ☐ By a non-unique identifier or other means. Please describe: N/A

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)**?** *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[8]	***N/A***
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)**?**	***N/A***

[6] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.
[7] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
[8] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[9]	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	Choose an item. Please describe applicable information sharing governance in place: **N/A**
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☒ No. What steps will be taken to develop and maintain the accounting: *Click here to enter text.* ☐ Yes. In what format is the accounting maintained: *Click here to enter text.*

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[10] ☐ Live PII data for testing ☒ No

[9] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.
[10] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[11] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

12. Does the planned effort include any interaction or intervention with human subjects[12] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[13]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*

[11] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;
(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—
(i) the detection of fraud, waste, or abuse in a Government agency or program; or
(ii) the security of a Government computer system.

[12] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[13] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

14. Is there a FIPS 199 determination?[14]	☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	A.L. Craig
Date submitted to Component Privacy Office:	July 8, 2021
Concurrence from other Component Reviewers involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	July 14, 2021

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

The Coast Guard is amending its rule on vessel financial responsibility to include tank vessels greater than 100 gross tons, clarify and strengthen the rule's reporting requirements, conform to current practice, and to remove two superseded regulations.

Responsible parties for certain vessels must establish and maintain evidence of financial responsibility, under both the Oil Pollution Act of 1990 (OPA 90), as amended, (specifically, 33 U.S.C. 2716) and the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (CERCLA) (specifically, 42 U.S.C. 9608). The evidence of financial responsibility must meet the maximum amount

[14] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

of liability under 33 U.S.C. 2704(a) or (d). Violators of those requirements are subject to various penalties under 33 U.S.C. 2716a and 42 U.S.C. 9609.

The 2010 Coast Guard Authorization Act (Public Law No. 111–281, 124 Stat. 2988 (October 15, 2010)) expands OPA 90 by adding any tank vessel greater than 100 gross tons but less than or equal to 300 gross tons using any place subject to U.S. jurisdiction to the population of vessels subject to the evidence of financial responsibility requirements. The Coast Guard is amending the Code of Federal Regulations (CFR) to reflect that statutory change.

The Coast Guard had previously issued Certificate of Financial Responsibility (COFR) regulations at 33 CFR part 138, subpart A, which apply to vessels over 300 gross tons, as well as certain other vessels depending on how and where they are operated. The Coast Guard has modernized and simplified its COFR program since those regulations were established. Certain aspects of the COFR program are improved, particularly in the COFR requirements for reporting changes in vessel operation, ownership, or evidence of financial responsibility that affected the basis of the Coast Guard's decision to issue a COFR. Finally, the structure of the COFR regulations and some of their provisions, including the rules for applying vessel gross tonnage, have been modernized to reflect changes in the law and Coast Guard practice, since OPA 90's initial legislation.

This rulemaking will ensure the Coast Guard has current information when there are significant changes in a vessel's operation, ownership, or evidence of financial responsibility, and reflect current best practices in the Coast Guard's management of the Certificate of Financial Responsibility program.

The Financial Responsibility – Vessels Superseded Funds not a privacy sensitive rule.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	***Kattina Do***
DHS Privacy Office Approver (if applicable):	*Riley Dean*
Workflow Number:	***0018740***
Date approved by DHS Privacy Office:	*July 14, 2021*
PTA Expiration Date	*July 14, 2024*

DESIGNATION

Privacy Sensitive System:	No
Category of System:	Rule If "other" is selected, please describe: *Click here to enter text.*
Determination:	☒ Project, Program, System in compliance with full coverage ☐ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	Choose an item. *Click here to enter text.*
SORN:	Choose an item. *Click here to enter text.*

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

USCG is submitting this PTA to discuss the Financial Responsibility-Vessels; Superseded Funds. The Coast Guard is amending its rule on vessel financial responsibility to include tank vessels greater than 100 gross tons, clarify and strengthen the rule's reporting requirements, conform to current practice, and to remove two superseded regulations. This rulemaking will ensure the Coast Guard has current information when there are significant changes in a vessel's operation, ownership, or evidence of financial responsibility, and reflect current best practices in the Coast Guard's management of the Certificate of Financial Responsibility program.This rulemaking will also promote the Coast Guard's missions of maritime stewardship, maritime security and maritime safety.

The DHS Privacy Office (PRIV) agrees with USCG Privacy that this rule is not privacy sensitive and a PTA is sufficient at this time.