



PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

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

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number: CG-6025A

Form Title: Vulnerability and Security Measures Addendum

Component: U.S. Coast Guard (USCG) **Office:** CG-REG

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title: Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements

OMB Control Number:	1625-0077	OMB Expiration Date:	November 30, 2022
----------------------------	-----------	-----------------------------	-------------------

Collection status:	Extension	Date of last PTA (if applicable):	July 25, 2019
---------------------------	-----------	--	---------------

PROJECT OR PROGRAM MANAGER

Name: Mr. David Du Pont

Office:	CG-REG	Title:	Reg Dev Mgr
----------------	--------	---------------	-------------

Phone:	202-372-1497	Email:	David.A.DuPont@uscg.mil
---------------	--------------	---------------	-------------------------

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name: A.L. Craig

Office:	CG-6P	Title:	PRA Coordinator
----------------	-------	---------------	-----------------

Phone:	202-475-3528	Email:	Albert.L.Craig@uscg.mil
---------------	--------------	---------------	-------------------------



SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

a. Describe the purpose of the information collection or form.

The U.S. Coast Guard (USCG) is renewing the Information Collection Request (ICR) titled, 1625-0077: "Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements."

The Vulnerability and Security Measures Addendum (CG-6025A) is used to document facility vulnerabilities and the security measures used to address the vulnerabilities. The Coast Guard uses this information to determine if facilities are in compliance with the maritime security requirements mandated by the Maritime Transportation Security Act of 2002 (MTSA). This form may only be used in addition to form CG-6025, never alone.

CG-6025A contains the name of the facility, facility vulnerability, facility vulnerability category, facility security measures, facility security measures category, and any amplifying facility information.

The Vulnerability and Security Measures Addendum (CG-6025A) is uploaded into the facility-specific file in the Marine Information for Safety and Law Enforcement system.

Records associated with this collection are maintained in accordance with NARA retention schedule number N1-026-05-015.

b. List the DHS (or Component) authorities to collect, store, and use this information.

46 U.S. Code 70103 is the authority for this collection.

2. Describe the IC/Form



a. Does this form collect any Personally Identifiable Information" (PII ¹)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
b. From which type(s) of individuals does this form collect information? (Check all that apply.)	<input checked="" type="checkbox"/> Members of the public <input checked="" type="checkbox"/> U.S. citizens or lawful permanent residents <input checked="" type="checkbox"/> Non-U.S. Persons <input type="checkbox"/> DHS Employees/Contractors (list Components) <input type="checkbox"/> Other federal employees or contractors
c. Who will complete and submit this form? (Check all that apply.)	<input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input checked="" type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input checked="" type="checkbox"/> Business entity. If a business entity, is the only information collected business contact information? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Law enforcement. <input type="checkbox"/> DHS employee/contractor. <input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. Please describe. Click here to enter text.
d. How do individuals complete the form? Check all that apply.	<input checked="" type="checkbox"/> Paper. <input checked="" type="checkbox"/> Electronic. (ex: fillable PDF) <input type="checkbox"/> Online web form. (available and submitted via the internet) Provide link:
e. What information will DHS collect on the form?	

¹ Personally identifiable information means 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.



CG-6025A contains the name of the facility, facility vulnerability, facility vulnerability category, facility security measures, facility security measures category, and any amplifying facility information.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? No.

- | | |
|---|--|
| <input type="checkbox"/> Social Security number | <input type="checkbox"/> DHS Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Alien Number (A-Number) | <input type="checkbox"/> Social Media Handle/ID |
| <input type="checkbox"/> Tax Identification Number | <input type="checkbox"/> Known Traveler Number |
| <input type="checkbox"/> Visa Number | <input type="checkbox"/> Trusted Traveler Number (Global Entry, Pre-Check, etc.) |
| <input type="checkbox"/> Passport Number | <input type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Bank Account, Credit Card, or other financial account number | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Other. <i>Please list:</i> | |

g. List the **specific authority** to collect SSN or these other SPII elements.

N/A

h. Is SSN necessary to carry out the functions of this form and/or fulfill requirements of the information collection?

N/A

i. How will this information be used? What is the purpose of the collection?

The Vulnerability and Security Measures Addendum (CG-6025A) is used to document facility vulnerabilities and the security measures used to address the vulnerabilities. The Coast Guard uses this information to determine if facilities are in compliance with the maritime security requirements mandated by MTSA. This form may only be used in addition to form CG-6025, never alone.

j. Are individuals provided notice at the time of collection by DHS (*Does the records subject have notice of the collection or is*

- ☐ Yes. Please describe how notice is provided.
Click here to enter text.
- ☒ No. Information is not retrieved by a personal identifier.



<i>form filled out by third party)?</i>	
---	--

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	<input type="checkbox"/> Paper. Please describe. Click here to enter text. <input type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form. Click here to enter text. <input checked="" type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Forms the Coast Guard receive are maintained in the Marine Information for Safety and Law Enforcement (MISLE) database.
b. If electronic, how does DHS input the responses into the IT system?	<input checked="" type="checkbox"/> Manually (data elements manually entered). Please describe. A scanned form is uploaded to the facility-specific file in MISLE. <input type="checkbox"/> Automatically. Please describe. Click here to enter text.
c. How would a user search the information submitted on the forms, <i>i.e.</i> , how is the information retrieved?	<input type="checkbox"/> By a unique identifier. ² Please describe. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. Click here to enter text. <input checked="" type="checkbox"/> By a non-personal identifier. Please describe. A search is accomplished using facility-specific information.
d. What is the records retention	A record is retained for the life of the facility; NARA retention schedule number N1-026-05-015.

² 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.



schedule(s)? <i>Include the records schedule number.</i>	
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	As records are maintained in the MISLE database, disposal/deletion is in accordance with the business rules for the database.
f. Is any of this information shared outside of the original program/office?	
<input type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.	
<input type="checkbox"/> Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe. Click here to enter text.	
<input checked="" type="checkbox"/> No. Information on this form is not shared outside of the collecting office.	



Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	A.L. Craig
Date submitted to Component Privacy Office:	July 29, 2022
Concurrence from other Components involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	September 7, 2022
Have you approved a Privacy Act Statement for this form? (<i>Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.</i>)	<input type="checkbox"/> Yes. Please include it with this PTA submission. <input checked="" type="checkbox"/> No. Please describe why not. Information is not retrieved by a personal identifier.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i>	
<p>The U.S. Coast Guard (USCG) is renewing the Information Collection Request (ICR) titled, 1625-0077: "Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements."</p> <p>The Vulnerability and Security Measures Addendum (CG-6025A) is used to document facility vulnerabilities and the security measures used to address the vulnerabilities. The Coast Guard uses this information to determine if facilities are in compliance with the maritime security requirements mandated by the Maritime Transportation Security Act of 2002 (MTSA). This form may only be used in addition to form CG-6025, never alone.</p> <p>CG-6025A contains the name of the facility, facility vulnerability, facility vulnerability category, facility security measures, facility security measures category, and any amplifying facility information.</p>	



The Vulnerability and Security Measures Addendum (CG-6025A) is privacy sensitive-coverage is provided by DHS/USCG/PIA-008, Marine Information for Safety and Law Enforcement.



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Brian Pochatila
PCTS Workflow Number:	0023114
Date approved by DHS Privacy Office:	September 8, 2022
PTA Expiration Date	September 8, 2025
DHS Privacy Office Approver (if applicable):	Schuntel Reddock

DESIGNATION

Privacy Sensitive IC or Form:	Yes If “no” PTA adjudication is complete.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input checked="" type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
Privacy Act Statement:	e(3) statement currently accurate. PN submitted and approved.
System PTA:	Choose an item. Click here to enter text.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) If a PIA update is required, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.



If a SORN update is required, please list: [Click here to enter text.](#)

DHS Privacy Office Comments:

Please describe rationale for privacy compliance determination above.

USCG is submitting this PTA renewal for the Information Collection Request (ICR) titled, 1625-0077: "Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements." The Vulnerability and Security Measures Addendum (CG-6025A) is used to document facility vulnerabilities and the security measures used to address the vulnerabilities. USCG uses this information to determine if facilities are in compliance with the maritime security requirements mandated by the Maritime Transportation Security Act of 2002 (MTSA). This form may only be used in addition to form CG-6025, never alone.

CG-6025A contains the name of the facility, facility vulnerability, facility vulnerability category, facility security measures, facility security measures category, and any amplifying facility information.

DHS Privacy concurs that the Vulnerability and Security Measures Addendum (CG-6025A) is privacy sensitive requiring PIA coverage. DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) covers information required to support the Coast Guard's marine safety, security, environmental protection and law enforcement programs.