The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt from the component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Date Submitted for Review: December 2, 2010

Name of Project: Port Stakeholder Interface Form

System Name in TAFISMA: N/A

Name of Component: United States Coast Guard

Name of Project Manager: Mr. Ryan Owens

Email for Project Manager: ryan.f.owens@uscg.mil

Phone Number for Project Manager: 202-372-1108

Type of Project:
☐ **Information Technology and/or System.***

☐ **A Notice of Proposed Rule Making or a Final Rule.**

☒ **Form or other Information Collection.**

☐ **Other: <Please describe the type of project including paper based Privacy Act system of records.>**

---

* The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).
- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note: for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

SPECIFIC QUESTIONS

1. Describe the project and its purpose:

According to Public Law 109-347 Sec 202, the Secretary of the Department of Homeland Security is directed to develop and update, as necessary, protocols for the resumption of trade in the event of a transportation disruption or a transportation security incident. Additionally, Homeland Security Presidential Directive (HSPD-13) identified the need for a Maritime Infrastructure Recovery Plan (MIRP). The MIRP is intended to protect the American economy by facilitating the restoration of passenger and cargo flow, specifically container cargo, in the event of an attack or similarly disruptive event.

In support of these directives, the Coast Guard, in conjunction with Customs and Border Protection developed a set of protocols designed to facilitate the expeditious recovery of trade. The protocols are predicated on a collaborative relationship with the maritime industry to assist the Coast Guard in identifying and prioritizing vessel traffic into an affected port. The process of this coordinating is enhanced by the inclusion of voluntarily submitted information from port facilities on the critical needs of cargo coming into the port.

The Port Stakeholder Interface Form is needed to facilitate the reception of port facility information regarding shipping and facility concerns and will be collected by the Coast Guard through an online form located on the Coast Guard's Homeport Internet Portal (http://homeport.uscg.mil).

The information collected will allow the Coast Guard to understand the cargo needs of the facilities within an affected port. This data will help the Coast Guard prioritize a vessel queue by identifying critical cargo needs.

2. Status of Project:

☒ This is a new development effort.

☐ This is an existing project.

Date first developed:

Date last updated:

<Please provide a general description of the update.>

3. From whom do you collect, process, or retain information on: (Please check all that apply)

☐ DHS Employees.

☐ Contractors working on behalf of DHS.

☒ The Public.

☐ The System does not contain any such information.

4. Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)

☒ No.

☐ Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so:

<Please provide the function of the SSN and the legal authority to do so.>

5. What information about individuals could be collected, generated or retained?

The Collection form requests a Point of Contact name, email, phone number and 24-hour contact phone number

6. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?

☒ No. Please continue to the next question.

☐ Yes. Is there a log kept of communication traffic?

☐ No. Please continue to the next question.

☐ Yes. What type of data is recorded in the log? (Please choose all that apply.)

☐ Header.

☐ Payload Please describe the data that is logged.

<Please list the data elements in the log.>

7. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[1]?

☒ No.

[1] 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 TAFISMA.

☐ Yes.

Please list:

8. Is there a Certification & Accreditation record within OCIO's FISMA tracking system?

☒ Unknown.

☐ 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

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

Date reviewed by the DHS Privacy Office: December 16, 2010

Name of the DHS Privacy Office Reviewer: Rebecca J. Richards

DESIGNATION

☐ **This is NOT a Privacy Sensitive System** – the system contains no Personally Identifiable Information.

☒ **This IS a Privacy Sensitive System**

Category of System

☐ IT System.

☐ National Security System.

☐ Legacy System.

☐ HR System.

☐ Rule.

☒ Other:

Determination

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ PIA is not required at this time.

☒ PIA is required.

☒ System covered by existing PIA: NOAD PIA

☐ New PIA is required.

☐ PIA update is required.

☐ SORN not required at this time.

☒ SORN is required.

☒ System covered by existing SORN: DHS/USCG-029

☐ New SORN is required.

DHS PRIVACY OFFICE COMMENTS