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: 11/23/10

Name of Project: Private Sector Clearance Program

System Name in TAFISMA: UNKNOWN

Name of Component: National Protection and Programs Directorate

Name of Project Manager: Monika L. Junker

Email for Project Manager: monika.junker@dh.gov

Phone Number for Project Manager: 703-603-5020

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

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

☒ **Form or other Information Collection.**

☐ **Other:**

---

* 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:

Protecting critical and key infrastructures requires cooperation between government and private industry. It is the policy of the Department of Homeland Security [DHS] to share pertinent information regarding infrastructure protection with the private sector, which at times must be classified information. The private sector official must be cleared for a federal security clearance prior to receiving classified information from the government. The Private Sector Clearance Program [PSCP] was developed to provide the means to accomplish the task of obtaining security clearances for the private sector officials. The Private Sector Clearance Program Roster (PSCPR) is used to track those Private Sector individuals involved in the clearance process.

This program is the liaison between the private sector individuals we need cleared and the DHS Office of Security whom clears them. The program's OMB-approved DHS Form 9014 is used to justify why the individual requires a clearance. This form requests information such as company name, job title, social security number, date of birth, place of birth, previous clearance (if applicable) and justification. We retain the original copy of the request form for our files and these files are kept in a locked cabinet at all times. The individual's information is placed on our roster for use in keeping track of individuals nominated and cleared, their clearance level, passing their clearance, etc. The information is only available for the Security Specialist working on the program. A sanitized roster is provided to DHS/NPPD personnel serving as either sector specialists, sector specific agency designated representatives, and protective security advisors on a quarterly basis (or upon request) for their routine use to perform their required duties of working with these individuals to execute the mission of infrastructure protection. The sanitized roster only includes first and last name, clearance level, which sector they are involved in, company, job title, the city and state they are located in, work e-mail address and work phone number. The rosters are provided to the Sector Specific Agencies, sector specialist and PSA in order for them to have access to private sector partners whom they can pass classified information to.

2. Status of Project:

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: approx 2004

Date last updated: 2010

In early 2010, the PSCP took on the responsibility of initiating e-QIP access and receiving the applicant's "package" (which only includes a set of completed/signed fingerprint cards, a credit release form and the certification/signature pages from e-QIP) to send to the Office of Security, Personnel Security Division for processing. This has streamlined the process as the PSCP now can track 100% of the packages, whereas previously the PSCP was not informed when packages were received (or not received) by the Office of Security.

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:

In order to process investigation requests through e-QIP and identify each person during the investigation/clearance process, SSN's are required. Section 201 of the Homeland Security Act; Executive Order 12968, and Executive Order 13526 (which replaced 12958) and authorizes the collection of this information

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

Legal name, date and place of birth, SSN, company employed by, job title, work address/e-mail/phone number, clearance level, and the CIKR sector they are associated with. If their clearance is adjudicated favorably, investigation type and date, as well as clearance date would also be generated and retained, both in the CIKR PSCP Master Roster and in ISMS, which is "owned" by the Office of Security.

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.

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

☐ No.

☒ Yes.

Please list: **After the applicant's package is received, it is sent to the Office of Security for processing. They input the information into ISMS, the DHS clearance database. (The applicant's background information is entered by the applicant into e-QIP, which is an OPM system.)**

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

[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.

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: November 24, 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:

☒ New PIA is required.

☐ PIA update is required.

☐ SORN not required at this time.

☒ SORN is required.

☒ System covered by existing SORN: DHS/ALL-023 - Department of Homeland Security Personnel Security Management

☐ New SORN is required.

DHS PRIVACY OFFICE COMMENTS