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, 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 DHSOnline 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)

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

SUMMARY INFORMATION

DATE **submitted for review:**

NAME **of** Project**: USCIS Transformation Project - Release A**

Name of Component: US Citizenship and Immigration Services

Name of Project Manager: Gregory L. Collett

Email for Project Manager: Greg.Collett@dhs.gov

Phone number for Project Manager: 202.233.2323

TYPE **of Project:**

☒ **Information Technology and/or System***

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

☐ **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:

USCIS is taking an incremental approach to Transformation, introducing limited new capability in stages called Releases in order to gradually transform the full operation. Deployment of Transformation is organized in two Increments encompassing five releases, by which transformed processes and capabilities are introduced in intervals. Increment 1 addresses the non-immigrant line of business (and a few immigrant and humanitarian benefit types) and transforms the vast majority of USCIS's systems and processes; Increment 2 addresses the remaining lines of business—immigrant, humanitarian, and citizenship.

Release A, therefore, is the first Release of Transformation and deploys the foundational capability that all subsequent releases will build on. The capabilities selected for Release A deliver specific business value to USCIS. A summary of the capabilities that will be provided in this release are depicted in the following paragraphs, organized by the five core management functions:

1. Immigration Account Management: Release A will allow individuals (such as customers and representatives) to establish and maintain individual accounts.

2. Benefits Case Management: The case management system includes automation of case intake (include benefit request data and fees), implementation of automated rule sets for completeness review, eligibility review, fraud and national security risk analysis, and system qualified adjudication when possible.

3. Electronic Content Management: USCIS may digitize the legacy paper A-file into Enterprise Document Management System (EDMS) and it will be linked to the customer account, enhancing the person-centric, account-based view. Additional services provided in Release A include producing notices and proofs of benefit on secure stock, cards or travel documents.

4. Agency and Knowledge Management: Release A will streamline and improve processes, capabilities, and data associated with managing Agency workload, resources, and performance; and the knowledge assets that support the Agency's work.

5. Risk and Fraud Management: Release A will introduce analytic processes and capabilities required to develop risk assessments for individual account holders and benefit-seekers and to discern and test new patterns suggestive of fraud and national security threats.

Benefit Request Types

Release A addresses some of the benefit types within the Non-Immigrant Line of Business. Data requirements that will be identified will include the data types necessary to fulfill the following activities and functions in Release A:

- Case History

- Background investigation data
- Criminal History information
- Biometrics
- Risk and Fraud Business rules
- Case data where benefits were denied
- Snapshots and audit trails

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. Could the project relate in any way to an individual?[1]

☐ No. Please skip ahead to the next question.

☒ Yes. Please provide a general description, below.

The system will request and collect Name, DOB, COB, COC, Gender, Alien Number, SSN, Address, Email Address, and Biometric data. Customers are classified into two categories: benefit seekers and non-benefit seekers. Benefit seekers include applicants (foreign national individual or family) or petitioners (Employer or Family sponsor). Non-benefit seekers are attorneys, representatives, school/officials, home study agencies, community based organizations, interpreters, preparers, DHS/CIS employees and contractors.

4. Do you collect, process, or retain information on: (Please check all that apply)

☒ DHS Employees

☒ Contractors working on behalf of DHS

[1] Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways. For example, a project that is focused on detecting radioactivity levels may be sensitive enough to detect whether an individual received chemotherapy.

☒ The Public

☐ The System does not contain any such information.

5. 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:

The collaboration mandated by The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208, dated September 30, 1996; Immigration Reform and Control Act of 1986 (IRCA), P.L. 99-603, dated November 6, 1986; and Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), P.L. 104-193, 110 Stat. 2168, dated August 22, 1996 to support the agency's verification activities requires the use of the Social Security Number (SSN) as a unique identifier to facilitate the verification

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

Name, Address, Date of birth, Citizenship, Gender, Country of birth, Social security number (if applicable), An email address, Biometrics, Background investigation data, Criminal history information, Risk and fraud business rules, Payment information, A-Numbers of the individual and close relatives and associates, receipt number, place of employment and employment history, family lineage, bank account information, marriage records, civil or criminal history information, education records.

7. 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.>

8. Can the system be accessed remotely?

☐ No.

☒ Yes. When remote access is allowed, is the access accomplished by a virtual private network (VPN)?

☐ No.

☒ Yes.

9. **Is Personally Identifiable Information[2] physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)**

☐ No.

☒ Yes.

10. **Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[3]?**

☐ No

☒ Yes. Please list:

The system will potentially receive data from Computer Linked Adjudication Information Management System (CLAIMS) 3, CLAIMS 4 and the Central Index Systems (CIS), EDIS and Lockbox and interface with eCISCOR, EDMS, PAS, Pay.gov and ICPS as well as ICE, CBP, DOS, DOJ, SSA, IRS, DOL, USVISIT

11. **Are there regular (ie. periodic, recurring, etc.) data extractions from the system?**

☐ No.

☒ Yes. Are these extractions included as part of the Certification and Accreditation[4]?

☐ Yes.

☒ No. The Certification and Accreditation will be completed before roll out of any system, but does not currently exist.

---

[2] Personally Identifiable Information is information that can identify a person. This includes; name, address, phone number, social security number, as well as health information or a physical description.
[3] 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.
[4] This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)

12. 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: April 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
- ☒ A PIA is required
  - ☐ System covered by existing PIA:
  - ☒ A new PIA is required.
  - ☐ A PIA Update is required.
- ☒ A SORN is required
  - ☐ System covered by existing SORN:
  - ☐ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS

SORN coverage to be fully determined via PIA process.