



Homeland Security

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
Version date: January 15, 2009

Page 2 of 7

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: Form I-9 Rulemaking

Name of Component: US Citizenship and Immigration Services

Name of Project Manager: Steven McHale

Email for Project Manager: steven.mchale@dhs.gov

Phone number for Project Manager: 202-358-7779

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:

The purpose of this project is to conduct a final rule-making for several changes to the Form I-9, "Employment Eligibility Verification Form". The Form I-9 is required by the Immigration Reform and Control Act of 1986, codified at 8 USC 1324a. It mandates that employees must fill out the Form and provide certain documents to an employer to verify the employees employment authority. The law requires the employer to maintain the completed Form I-9 for a certain period and to produce the Form if demanded by certain authorized government officials.

There have been several rulemakings for the Form I-9 dating back to 1987 and most recently an Interim Final Rule (IFR) was published December 17, 2008, 73 FR 76505. Although, there have been rulemakings since the Immigration and Naturalization Service (INS) became the Department of Homeland Security (DHS), there has been no Privacy Impact Assessment as required by Section 222 of the Homeland Security Act.

The changes proposed in the December 2008 IFR are to be finalized in the Final Rule that is the subject of this Privacy Threshold Analysis. The changes described in the IFR include modifications to the list of acceptable documents and receipts to establish identity and employment authority and technical changes to the Form I-9 and instructions. The rule proposed changing the requirement so that some documents, such as a United States passport, must now be unexpired. It discussed revising the language for Temporary Form I-551s, adding references to Form I-94A, and removing references to Forms I-688, I-688A, and I-688B. It also discussed making some technical corrections to based on changes to the law including changing references from INS to DHS and other minor changes.

It is significant to note that the Forms I-9 are not collected by the Federal government except in certain defined cases of investigations. So the collection, maintenance, and retention that are discussed are the collection, maintenance, and retention by the employer.

2. Status of Project:

This is a new development effort.

This is an existing project.

Date first developed: November 6, 1986

Date last updated: December 12, 2008

This Final Rule will make the following changes to the Form I-9. The Rule requires that some documents, such as a United States passport, must now be unexpired. It revises language to clarify that the Temporary Form I-551s may be a machine



Homeland Security

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
Version date: January 15, 2009

Page 4 of 7

readable form as well as a stamp. It adds references to Form I-94A, removes references to Forms I-688, I-688A, and I-688B. It also makes some technical corrections to based on changes to the law including changing references from INS to DHS and other minor changes.

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.

All employees that work in the U.S. whether citizens or not, are required to complete this form. The form is retained by the employer for three years from employee hire date or until one year after the date employment ends, whichever is later.

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

DHS Employees

Contractors working on behalf of DHS

The Public

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 SSN is an optional field on the Form I-9 unless the employer participates in the E-Verify Program. When the SSN is collected by the employer it is used to establish an employee's employment authority.

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

The Form I-9 asks for the employee's name, signature, address, date of birth, SSN (optional unless an E-Verify employer), citizenship status, and the document(s) title, issuing authority, document number, and expiration date for the documents

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.



Homeland Security

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
Version date: January 15, 2009

Page 5 of 7

presented by the employee for verification. The Form also contains the employer's name, signature, title, and business. And if the Form was prepared or translated by someone other than the employee, it will include the name, signature, and address of the preparer or translator.

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.

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

Yes

No

10. Is Personally Identifiable Information² physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)

No.

Yes.

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.



Homeland Security

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
Version date: January 15, 2009
Page 6 of 7

11. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems?

No

Yes. Please list:

12. Are there regular data extractions from the system?

No.

Yes. Are these extractions included as part of the Certification and Accreditation³?

Yes.

No.

13. 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

³ This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)



PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: March 27, 2009

NAME of the DHS Privacy Office Reviewer: Nathan Coleman, Acting Director Privacy Compliance

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

Whether a SORN is required will be determined upon drafting of the PIA.