Privacy Impact Assessment Update
for the

Electronic Filing System (e-Filing)

DHS/USCIS/PIA-024(a)

December 26, 2013

Contact Point
Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
202-272-8000

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) developed the Electronic Filing System (e-Filing) to allow individuals to securely apply for immigration benefits online. e-Filing is a customer service, web-based initiative developed to provide a mechanism for individuals to submit and track the processing of certain USCIS applications and petitions. USCIS is updating the e-Filing Privacy Impact Assessment (PIA) originally published on August 24, 2009 to include the collection and use of Internet Protocol address and browser information as part of detecting, pursuing, and deterring immigration benefit fraud.

Introduction

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States. USCIS is responsible for the administration of immigration and naturalization adjudication functions, and for establishing immigration services, policies, and priorities. In executing its mission, USCIS performs functions that include the adjudications of immigrant visa petitions; non-immigrant visa petitions, which are petitions filed by persons staying in the United States temporarily for a limited purpose (e.g., work); asylum and refugee applications; and naturalization applications. USCIS developed the Electronic Filing System (e-Filing) to allow individuals to securely apply for immigration benefits online.

e-Filing is a web-based tool that supports USCIS mission efficacy and efforts towards greater public transparency by providing a mechanism for individuals (applicants) or authorized parties acting on behalf of individuals (representatives) to submit applications and petitions (applications) for certain immigration benefits and services directly to USCIS. Currently, the forms below are available for e-Filing[1]:

- I-90, *Application to Replace Permanent Resident Card*
- I-765, *Application for Employment Authorization*
- I-131, *Application for Travel Document*
- I-140, *Immigrant Petition for Alien Worker*

[1] Separate from e-Filing, USCIS is transforming its operations by creating a new electronic environment known as the USCIS Electronic Immigration System (USCIS ELIS), which allows individuals requesting a USCIS benefit to register online and submit certain benefit requests through the online system. USCIS ELIS also allows immigration benefit seekers and their legal representatives to create an account and file benefit requests online. Only certain applicants (Form I -539 and Immigrant Fee) can electronically file online. Over time, USCIS ELIS will include more benefit types and increased functions.

- I-821, *Application for Temporary Protected Status*
- I-907, *Request for Premium Processing Service*
- G-28, *Notice of Entry of Appearance as Attorney or Representative*

USCIS uses e-Filing because the system eliminates the need for certain applications to be submitted to USCIS in hard-copy and then manually inputted into the Computer-Linked Application Information Management System 3 (CLAIMS 3) by data entry staff.[2] USCIS requires applicants and representatives to register and create unique user accounts to access e-Filing. By creating an e-Filing account, applicants and representatives are able to submit forms electronically and retain partially completed forms in his or her account for future use. If the customer chooses to create an account, he or she must first affirmatively agree to adhere to the e-Filing Privacy Policy prior to establishing an account. The e-Filing Privacy Policy informs applicants and representatives that e-Filing automatically collects and stores certain technical information (e.g., Internet Protocol (IP) address,[2] internet domain, type of browser) during each browser session in addition to account creation and benefit application information. In addition, when the customer logs into e-Filing, USCIS automatically collects and stores certain browser information in server logs. A server log is a log file automatically created and maintained by a server of activity performed by the user. The purpose of the server log is to keep track of and monitor what is happening with the server. These files are only accessible to the e-Filing Administrator.

e-Filing collects information directly from the applicant and his or her representative. Every application package, regardless of the benefit sought, must include complete information in all required blocks of the form, all supporting documents, a signature, and the correct fee. USCIS uses the information submitted to assist USCIS adjudicators in corroborating information provided by applicants, thereby ensuring that the process is consistent with applicable laws and regulations. This information is also used to perform background checks, to review the information that is being provided by applicants, and to adjudicate applications. Information in e-Filing is subject to a 15-year retention period.

Reason for the PIA Update

The USCIS Fraud Detection and National Security Directorate (FDNS) is responsible for preserving the integrity of the U.S. immigration system by detecting and

[2] See DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) for more information, available at www.dhs.gov/privacy.
[2] An IP address is a number that is automatically assigned to a computer when connected to the Internet.

deterring immigration benefit fraud.[3] Adjudicators may refer e-filings suspected of fraud to FDNS throughout the application process. FDNS conducts administrative inquiries into suspected benefit fraud and aids in the resolution of these cases. FDNS Immigration Officers (IO) may collect evidence from a variety of sources during an administrative inquiry. For example, FDNS may request a user's IP address and browser information associated with an electronically filed case to assist with identifying a potentially fraudulent application and determining the geographic location of suspects. Various fraud indicators must be present before FDNS requests the IP address for a particular application.[4]

USCIS is updating the existing e-Filing PIA to describe the use of Internet Protocol (IP) addresses and above-described session information for use in administrative fraud investigations. An IP address is a unique network identifier issued by an Internet Service Provider to a user's computer every time they are logged on to the Internet. There are many details associated with an IP address. These details include the host name and geographic location information (e.g., country, region/state, city, latitude, longitude, telephone area code). E-Filing automatically captures and stores the IP address and browser information when the user logs into e-Filing.

When someone completes and submits an application through e-Filing, they are given an electronic confirmation receipt number after which that receipt number is linked to a customer user account along with session information.[5] USCIS uses the receipt number to retrieve the customer, account, and session data from e-Filing and its audit logs: session ID, user ID, e-mail address, physical address, last name, first name, telephone number, time of submission, date of submission, payer name, payment method, amount paid, and form type. FDNS analyzes this information to assist with fraud investigations.

FDNS uses a variety of sources, including IP address information when investigating fraud. While FDNS does not use IP address as the sole means of determining the geographic location of an applicant or representative, it may be used to validate or lead FDNS to other information to use in the course of its investigation. If there is an indication of possible fraud, national security, or public safety concerns.

[3] See DHS/USCIS/PIA-013(a) – Fraud Detection and National Security Directorate for more information, available at www.dhs.gov/privacy

[4] Fraud indicators may include, inconsistent name matches in DHS systems, multiple filings, common addresses on different applications, and suspect documents (i.e., altered or counterfeit documents).

[5] e-Filing displays a Confirmation Receipt Number, a link to a PDF version of the form the individual filed, and a Confirmation Receipt Notice. Within 10 days of filing, USCIS also mails the individual Form I-797, Notice of Action, which lists the Confirmation Receipt Number.

FDNS may proactively share information with other government entities as described under the DHS/USCIS-006 FDNS-DS System of Records Notice (SORN).[6]

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

USCIS is amending Section 1 of the DHS/USCIS/PIA-024 e-Filing to include the collection and storage of IP address and session information. e-Filing is a service that allows customers to complete and submit applications electronically. During an active browser session, e-Filing automatically collects and stores certain technical information. This information includes: internet domain, IP address (an IP address is a number that is automatically assigned to a computer when surfing the Internet), type of browser, operating system used to access our site, date and time the site was accessed, and visited pages.

Uses of the System and the Information

e-Filing is an online tool that allows USCIS applicants to securely apply for immigration benefits. USCIS continues to use the information to administer and adjudicate benefits as described in Section 2.0 of DHS/USCIS/PIA-024 e-Filing. FDNS may request and use session information associated with a potentially fraudulent application from e-Filing. However, session information from the server logs is only accessible to and must be retrieved from the System Administrator.

The 15-year retention schedule provides FDNS with access to information that is critical to the investigation of suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns.

FDNS forwards the e-Filing System Administrator the following customer details: session ID, user ID, e-mail address, last name of user, first name of user, telephone number of user, time of submission, date of submission, payer name, payment method, amount paid, and form type to initiate a request for browser information. The e-Filing System Administrator uses this information to retrieve associated browser information, including IP address by searching through session logs. The System Administrator electronically returns the browser information to FDNS via spreadsheet. The browser information provided to FDNS will be compared to other evidence collected during the administrative inquiry. After reviewing all of the information collected throughout the

[6] See DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411.

administrative inquiry, FDNS makes a fraud determination based on the totality of all the evidence collected, not solely based upon the person's IP address.

Retention

An application used in connection with a fraud, public safety, or national security concern will be retained for 15 years from the date of the last interaction between FDNS personnel and the applicant after which time the record will be deleted from FDNS. Upon closure of a case, any information that is needed to make an adjudicative decision, such as a statement of findings report, whether there was or was not an indication of fraud, criminal activity, egregious public safety, and/or national security concerns, will be transferred to the A-File and maintained under the A-File retention period of 100 years after the applicant's date of birth.

Internal Sharing and Disclosure

The internal sharing and disclosure of information has not changed with this update. USCIS will continue to share information with to DHS Components to support of research into e-Filing system misuse or broader fraudulent activity affecting USCIS as described in DHS/USCIS/PIA-024 e-Filing.

External Sharing and Disclosure

The external sharing and disclosure of information has not changed. USCIS will continue to share information with non-DHS as described in DHS/USCIS/PIA-024 e-Filing.

Notice

This PIA Update provides applicants and representatives with notice of the updated uses described in this PIA. Notice is also provided in the DHS/USCIS/007-Benefits Information System (BIS) SORN, September 29, 2008, 73 FR 56596, and by DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS) SORN.[7] Additionally, USCIS notifies applicants and representatives that e-filing automatically collects IP addresses and browser information through its Privacy Policy.

Individual Access, Redress, and Correction

Because FDNS contains sensitive information related to possible immigration benefit fraud and national security and/or public safety concerns, DHS has exempted FDNS from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(k)(2). Notwithstanding the applicable exemptions, USCIS reviews all such requests on a case-by-case basis. Where such a request is made, and access would not appear to interfere with or adversely affect the national or

[7] DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411.

homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORN.

Any applicant seeking to access information maintained by USCIS should direct his or her request to:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Requests for access to records must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity in accordance with DHS regulations governing Privacy Act requests (found at 6 CFR § 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may be exempt from disclosure under the Privacy Act because FDNS records, with respect to an applicant, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations. Additional information about Privacy Act and Freedom of Information Act (FOIA) requests for USCIS records can be found at http://www.uscis.gov.

Technical Access and Security

The technical access and security controls for e-filing have not changed with this update. USCIS continues to employ criteria, procedures, controls, and responsibilities regarding e-Filing security and technical access as outlined in the DHS/USCIS/PIA-024 e-Filing.

Technology

The technical access and security controls for e-Filing have not changed with this update.

Responsible Official

Donald K. Hawkins
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security