Privacy Impact Assessment
for the

Electronic Filing System
(e-Filing)

August 24, 2009

Contact Point
Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
202-272-1400

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780
Abstract

The United States Citizenship and Immigration Service (USCIS) has developed the Electronic Filing System (e-Filing). 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 has developed this Privacy Impact Assessment (PIA) to document, analyze, and assess current USCIS practices with respect to the collection, use, and sharing of personally identifiable information (PII) and the implementation of e-Filing.

Overview

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 adjudications of:

- immigrant visa petitions;
- non-immigrant visa petitions (petitions filed by persons staying in the US temporarily for a limited purpose [e.g., to work]);
- asylum and refugee applications; and
- naturalization applications.

E-Filing is a web-based tool that supports USCIS mission efficacy and efforts towards greater public transparency by providing a mechanism for individuals or authorized parties acting on behalf of individuals (referred to herein collectively as “applicants”) to submit applications and petitions (referred to herein collectively as “applications”) for certain immigration benefits and services directly to USCIS. E-Filing eliminates the need for some applications to be submitted to USCIS in hard-copy and then manually input by USCIS staff into the CLAIMS system. (E-Filing is not a case management system.)

Data submitted to USCIS through e-Filing is used to assist USCIS examiners in corroborating information provided by applicants, thereby ensuring that the process is consistent with all applicable laws and regulations. This data is used to perform background checks, examinations (review of the information that is being provided by applicants), and adjudications (process by which decisions are made to grant or deny an application).

A typical transaction conducted in the system begins when an applicant initiates a request for a user account. From this page the e-Filing user may either log directly into his/her account or select to create a new account.

---

1 The electronic storage of information in CLAIMS is outlined in the System of Records Notice in the Federal Register (http://edocket.access.gpo.gov/2008/E8-22802.htm). The e-Filing system is one of several initiatives that support and address the strategies and elements of the USCIS strategic goals outlined in the Immigration Services Program Business Plan 2002-2012.
New users must affirmatively agree to adhere to the e-Filing Privacy Policy prior to establishing an account. The Privacy Policy used by the e-Filing System is consistent with this PIA and will be updated as necessary to accurately reflect the information collected and the uses of that information.

After creating a user account, the user will then complete the form appropriate for the USCIS benefit sought. Because some applications require a fee payment, payment information is sent to the Department of Treasury’s Pay.gov system (see Financial Management Service (FMS) PIA and Revenue Collection Records – Treasury/FMS.017 SORN, 68 FR 5691 published on February 4, 2003), which acts as the clearing house to collect and process automated clearing house and credit-card information provided by the e-Filer.

The user is able to select from among the eight benefits forms available for e-Filing. The e-Filing System provides a question and answer format for users to follow to complete the form data; this provides a user-friendly interface that helps guide applicants in the accurate entry of form data. As the user progresses through the application process, the e-Filing System automatically saves the user’s data as the user navigates from screen to screen. The e-Filing System will store up to 20 not yet-submitted forms at a time, enabling the user to begin an application and return to it at a later time for payment and submission.

To complete the application process the user must enter valid data into all required fields, pay for the fees associated with the application(s), and certify that the information that has been submitted is accurate. After submitting the form data, the user will not be able to access or make edits to the submitted form or data via the e-Filing System; please see Section 7.0 of this PIA for how these actions are accommodated for e-Filing data. In addition, the e-Filing System does not provide any further information regarding the status of the application’s adjudication, since application adjudication occurs completely outside the scope of e-Filing.

Once the e-Filing System has collected the submitted data from the user, the e-Filing System transmits the data to the appropriate benefits administration system. Currently, all data is transferred to the appropriate CLAIMS3 LAN at either a Service Center or the National Benefits Center (NBC).

The e-Filing System was created in response to mandated legislative deadlines, including the Government Paperwork Elimination Act (GPEA). The e-Filing system has been implemented using a phase approach. Significant functionality provided by e-Filing includes:

- Allowing for the registration and association of PINs and passwords to applications prior to access and final submittal from the Internet or World Wide Web (Web) interface;
- Allowing for email of registered user account information (excluding sensitive PIN/Password information) to registered users electronically;
- Allowing for the I-90, I-129, I-131, I-140, I-539, I-765, I-821, and I-907 applications to be filed electronically (see Section 1.1 for details on these forms);
- Allowing for electronic validation and submission of completed applications and concurrently filed applications filed over the Web;
- Allowing for electronic submission of fee payments with automated clearing houses or credit card accounts;
- Allowing for an electronic receipt for fee payment and application submission through a Confirmation Receipt notice, which is provided for each e-filed application using the
Receipt Number;

• Enabling the tracking of the status of each e-filed application throughout the process;
• Enabling electronic transmission and routing of e-Filing data to the appropriate CIS case management system;
• Allowing for the updates of production tables (e.g., Temporary Protected Status (TPS), classifications based on cap counts, and application fees) and the generation of reports (e.g. summary reports, aging reports, eligibility code reports, settlement or activity reports, error reports, etc.) based on user roles, functions, and privileges;
• Allowing for the submittal of concurrently e-filed applications; and
• Allowing for the administration of user accounts and intranet user identifications and passwords based on user roles, functions, and privileges.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

E-Filing System allows users to establish unique user accounts, enabling the users to complete and pay for benefits forms, and transfers application data to the appropriate benefit adjudication system.

Establishment of an e-Filing account requires users to provide the following data elements:

• Name (first and last);
• Organization Name (required if the e-Filer is acting on behalf of another individual);
• User ID and Password (self-selected identifier used for future access to e-Filing in combinations with a self-selected confidential alpha-numeric special character string);
• Password Hint and Response (pre-identified list of questions and self-selected response to selected hint question);
• Email Address;
• Physical Address (street number and name, city/town, state/providence, country, and postal code);
• Telephone Number; and
• Date of Birth.

E-Filing collects information directly from applicants based on the specific form(s) selected from the menu of available applications (I-90, Application to Replace Permanent Residence Card; I-129, Petition
for Nonimmigrant Worker and I-129S, Nonimmigrant Petition Based on Blanket L Petition\(^2\); I-131, Application for Travel Document; I-140, Immigration Petition for Alien Worker; I-539, Application to Extent Temporary Stay; I-765, Application for Employment Authorization; I-821, Application for Temporary Protected Status; and I-907, Request for Premium Processing Service). The following information derived from these forms varies and not all forms collect the same information:\(^3\)

- **Names:** USCIS collects names (First, Last and Middle) for applicants, petitioners (employer or individual filing for their spouse or children), beneficiaries (worker, dependent, fiancé/spouse, or child), mother’s/father’s first name and attorneys/representatives;
- **Addresses:** USCIS collects addresses of applicants, petitioners and petitioner’s attorney/representative;
- **Telephone Numbers:** USCIS collects telephone numbers (applicant’s phone number);
- **Birth Information:** USCIS collects birth dates (applicant, petitioner, spouse, children/stepchildren/adopted children, fiancé);
- **Social Security Numbers:** USCIS collects Social Security Numbers (applicant, fiancé, and spouse) in certain forms;
- **Citizenship/Nationality Information:** USCIS collects citizenship information (country of nationality, country of citizenship, and country of birth) in certain forms;
- **Information Regarding Immigration Status:** USCIS collects information regarding immigration (current/ spouse’s immigration status, applicant’s, children’s and spouse’s Alien Numbers) and entry to the U.S. (days spent outside the U.S., dates of entry, port of entry, immigration status expiration dates, destination in the U.S.);
- **Marital Status:** USCIS collects information regarding marital (i.e., whether applicant is married, single, widowed or divorced.); and
- **Tax, Financial, and Payment Information:** USCIS collects tax identification numbers and Financial/Payment information (check information, bank account numbers, credit card numbers (the last four digits only) and other payment information).

### 1.2 What are the sources of the information in the system?

Information submitted to USCIS via e-Filing comes directly from the applicant.

To support e-Filing automated data validation processes, the e-Filing System contains information

\(^2\) I-129S is currently disabled in the e-Filing system.

\(^3\) The data collected and transmitted through the e-Filing systems reflects the data collected on the OMB-approved form; in some instances, the e-Filing system must collect additional information from applicants in order to facilitate system processing and/or application routing requirements.
obtained from sources other than the individual applicant. Two such scenarios are the validation of eligible I-907 cases and validation of zip codes.

The data imported into e-Filing to support eligible I-907 cases is based on data stored in CLAIMS 3. A I-907, Request for Premium Processing Service, may be filed for certain types of benefits applications, based on business rules and the application’s current status in CLAIMS 3. To prevent ineligible filings of the I-907, the e-Filing System imports data from CLAIMS 3 that summarizes all cases eligible for Premium Processing. The e-Filing System then checks this list to ensure the receipt number selected for upgrade with an I-907 application is eligible.

E-Filing also uses data imported from United States Post Office (USPS) to update the system with the latest zip codes, ensuring that user-entered combinations of city/state/zip code are valid. This system check ensures a higher degree of accuracy in the collection of addresses.

The e-Filing system is designed to collect information from various external user groups who are acting on behalf of applicants as well as directly from applicants. Figure 1: e-Filing User Group Profile outlines typical e-Filing users.

<table>
<thead>
<tr>
<th>User Group</th>
<th>Typical Reason For Filing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td>Individual customers seeking immigration benefits who access the e-Filing system without aid.</td>
</tr>
<tr>
<td>Community-Based Organizations (CBOs) and other Assistance-based entities</td>
<td>CBOs and other Assistance-based organizations provide individual customers with assistance in navigating the USCIS’ application processes. These organizations may assist individual customers in accessing the e-Filing system through the use of their computers and provide assistance in filling out the on-line form, as well as provide assistance to individual customers in making fee payments on-line by paying with the organization’s credit card in exchange for cash for the fees.</td>
</tr>
<tr>
<td>Lawyers &amp; Law Firms</td>
<td>Lawyers and law firms provide legal assistance to both individual customers and businesses. They may assist the individual customer or company in filling out the form itself or providing legal advice as to how to properly fill out the form.</td>
</tr>
<tr>
<td>US Businesses</td>
<td>US Businesses that hire foreign nationals to work inside the US fill out applications to sponsor their employee or assist their employee in completing applications.</td>
</tr>
<tr>
<td>Foreign Governments</td>
<td>Foreign Governments that send non-immigrants to the US for official government business may assist their employee in completion of application and/or provide facilities and other types of assistance to support the application submittal process.</td>
</tr>
</tbody>
</table>

E-Filing does not contain information obtained from public websites, data brokers, commercial aggregators and/or other private entities.
1.3 Why is the information being collected, used, disseminated, or maintained?

All information collected from e-filers seeking benefits is necessary to establish an e-Filing account and/or establish the e-filer’s identity and history with USCIS; to determine eligibility for the benefit sought; and to perform necessary background and security checks.

1.4 How is the information collected?

E-Filing allows for the secure electronic filing of USCIS applications for a limited number of USCIS applications forms, which allows USCIS to push the information from the e-Filing form directly into USCIS or other appropriate systems.

1.5 How will the information be checked for accuracy?

USCIS will rely on the following measures to promote the accuracy of the information it utilizes:

- The accuracy of application information submitted to USCIS by e-filers will be initially based on the accuracy of application information submitted by the e-filer at the time of submission through the on-line tool. Individuals who apply for benefits have personal incentive to submit accurate information.

- The system generates and maintains data quality metrics which will be used to identify problematic trends for remediation.

E-Filing contains automated business rules that alert E-filers at the time of data entry when information entered into certain fields is inconsistent, and provides instructions for resolving these inconsistencies. The e-Filing system is designed to perform minimal checks on collected data to ensure validation, accuracy, and completeness. These checks include:

- **Edit Checks** – The system performs edit checks on specific data fields to ensure a valid data value is provided (e.g., City, State, and Zip Code validation).

- **“Required” Data Field Notations** – The system denotes required data fields with an asterisk (*) and the system will not allow the applicant to proceed to the next screen until the data field is populated.

- **Warning Message** – The system automatically displays a message to the applicant when he/she fails to provide information in a “non-required” data field.

- **Error Message** – The system automatically displays a message to the applicant when he/she fails to provide information in a “required” data field.

USCIS treats all requests for corrections as Privacy Act requests. If upon later review an applicant determines that information in the system is incorrect, the individual should submit a Privacy Act request as

4 These data checks will help identify some errors due to data entry but will not be able to catch all errors. For example, the system will recognize as invalid a phone number that includes an alphabetic character but will not be able to identify a 10-digit phone number that was entered incorrectly.
described under Section 7.1 of this document. While the user will not be able to update the information directly into the e-Filing System, USCIS will be able to make the appropriate updates in the case management system of record.

In addition to these protections, the accuracy of the data entry can also be challenged during the appeals process if a petition is denied or during the interview process when required.

Information collected via e-Filing is also checked for accuracy through database technical controls, inherent business logic built into the system, and a manual review process (e.g., interviews with the applicants). Improved processes are being put in place for periodic review of personally identifiable information (PII) contained in the system to ensure it is timely, accurate, and relevant as required by the Office of Management and Budget (OMB) and the Privacy Act of 1974.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The primary legal authority supporting the collection of the information for USCIS forms is 8 U.S.C. § 1101 et seq. More specifically, 8 U.S.C. §1103 charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens. The DHS Secretary has delegated these duties to the USCIS Under Secretary pursuant to a Departmental management directive. In addition, the OMB has approved the content and format of every public form used by USCIS. The e-Filing System was also designed to comply with the measures detailed in the Government Paperwork Elimination Act (GPEA).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Inherent in all data collection activities is the risk of data collection in excess of defined business needs and use.

Mitigation: USCIS limits the information collected in e-Filing to that which is necessary to process or adjudicate immigration petitions and applications. Different sets of information are collected for each immigration benefit sought, and this set of information is based on the minimum necessary to process the benefit. The only PII stored in these systems is information entered by applicants which is necessary to use the system or to obtain the USCIS benefit.

USCIS further limits the possibility of unnecessary and burdensome data collection from applicants by adherence to the Paperwork Reduction Act (PRA) which requires that the Office of Management and Budget (OMB) approve all forms used for the collection of information from members of the public. OMB has approved the base forms from which e-Filing data collection requirements are drawn. USCIS provides interested parties with links to PRA statements that will be reviewed by OMB on its website – www.uscis.gov.

Privacy Risk: There is a risk of inaccurate information within E-filing system.

Mitigation: Generally, e-Filing relies on the accuracy of application information collected directly
from the applicant. Individuals who apply for benefits have the incentive to submit accurate information. If, however, it is determined that the system does contain incorrect information (e.g., because of a transcription error or incorrect information provided by the applicant), the applicant may correct information by contacting USCIS and submitting a Privacy Act request for correction.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

All of the information in Question 1.1 is used to:

- correctly record and identify the applicant and to verify the accuracy of information provided in an application (including the information of spouses and dependents),
- send correspondence (e.g., denial, grant and/or requests for additional information) to the applicant or other persons relevant to the application process, and
- verify with the applicant any assistance received in the completion of the application to assist in tracking and investigating preparer fraud.

The payment data collected via the e-Filing system is used by the Department of Treasury’s Pay.gov system to settle payments for application and biometric services fees. Payment data is not stored in the e-Filing system and payment account information (account numbers, routing numbers) cannot be viewed by internal USCIS users in the e-Filing system. Once the payment data is transmitted through the e-Filing system to Pay.gov, users at the USCIS Debt Management Center (DMC) can view payment details using the Department of Treasury’s Pay.gov system reporting tools. DMC must view these payment details in order to process the payment. DMC has access controls on what employees can access what level of payment information. Aces is confined to DMC employees in a need to know.

2.2 What types of tools are used to analyze data and what type of data may be produced?

USCIS does not use e-Filing account creation data or information submitted to perform complex analytical tasks resulting in data matching, relational analysis, scoring, reporting, or pattern analysis.

The system itself does not make available new or previously unavailable data from newly derived information. USCIS human analysts do, however, collect data from applicants and compare that data to other sources of information to assess whether the applicant is entitled to the benefit sought (see Sections 1.3, 4.0, and 5.1 in this document). While the outcome of this analysis is placed in the applicant’s record, USCIS does not use the e-Filing System to adjudicate or analyze applications; e-Filing is merely an intake and communication system.
2.3 If the system uses commercial or publicly available data please explain why and how it is used.

USCIS does not use commercially or publicly available data in support of e-Filing functionality.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: There is a risk that users who have access to the information will use the information in unauthorized manners.

Mitigation: DHS Management Directive System (MD) Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, May 11, 2004, provides guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. Additionally, all DHS employees are required to take annual computer security training, which addresses this issue.

DHS also maintains Rules of Behavior for employees who use DHS systems. Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines are established to hold users accountable for their actions and responsible for IT security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. OMB Circular A-130 requires that all major applications and general support systems have Rules of Behavior. e-Filing System users are required to read and sign the Rules of Behavior prior to receiving access to the system. A record of those users who have signed is maintained by the ISSO. Disciplinary action can be taken for violating the Rules of Behavior. The e-Filing System Rules of Behavior conform with 4300A DHS Sensitive Security Handbook - Rules of Behavior.

Any person who is in non-compliance with the rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

Users are presented the DHS guidelines for corporate Rules of Behavior when completing the mandatory security application for access to the e-Filing System. Users acknowledge they have read, understood, and agreed to the content of these rules. These rules cover system access, passwords and other access control measures, data protection, use of government office equipment, software, internet and e-mail use, incident reporting, and accountability. They acknowledge, by signing and dating the DHS Rules of Behavior that violating the system rules of behavior will involve potential disciplinary actions.
Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

### 3.1 How long is information retained?

All e-Filing application data is retained in immediately accessible form during the application processing timeframe. All e-Filed application data is maintained as received (i.e., the original information is not overwritten). Except for those cases adjudicated electronically, USCIS prints the data from the e-Filing System and includes the printout with the hard-copy file for adjudication.

At the time of creation of this PIA, no e-Filing data has been purged from the system. Upon the approval of a retention schedule by NARA, the data no longer necessary for storage will be removed from the e-Filing System. It is anticipated that e-Filing will retain records for no longer than 15 years.

E-Filing transmits relevant information and application and payment information to CLAIMS 3. Information located on the CLAIMS 3 system is archived and disposed of in accordance with the criteria approved by the National Archives and Records Administration (NARA). The CLAIMS 3 retention schedule is outlined in the USCIS CLAIMS 3 PIA.5

E-Filing passes payment information to the Department of Treasury’s Pay.gov system which acts as the clearing house to collect and process automated clearing house and credit card information provided by the e-filer.

All Personal Identification Number (PIN) and Password data from applicants is recorded in audit logs. While the PIN and Password do not expire, the user’s Password must be updated on a regular schedule to comply with system security requirements in order to have continued use of the e-Filing System.

### 3.2 Has the retention schedule been approved by the component records officer and NARA?

USCIS has developed a records retention schedule for e-Filing to comply with National Archives Records Administration (NARA) standards and has submitted this schedule to NARA for review.

For some benefit applications submitted through e-Filing, USCIS retains a hardcopy of the benefit application data when the e-Filed submission is complete. The retention period for hard copy files is established in the NARA schedule for the OMB approved USCIS forms associated with e-Filing collections.

5 Please see “USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum,” September 5, 2008; this file is located at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.
3.3 **Privacy Impact Analysis:** Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

**Privacy Risk:** There is a risk that information could be maintained for a period longer than necessary to achieve agency objectives.

**Mitigation:** Although there is always risk inherent in retaining data for any length of time, e-Filing data retention periods are consistent with the concept of retaining data only for as long as necessary to support the agency’s mission. The schedule proposed and approved by NARA matches the requirements of the Federal Records Act and the stated purpose and mission of the system. The time periods in the NARA schedule were carefully negotiated between USCIS and NARA to ensure that data is retained for the minimum time needed to process the application and make the information available for other USCIS benefits that might be sought by an applicant.

Information collected through e-Filing and ultimately stored in other USCIS systems or the Department of Treasury’s Pay.gov systems will be retained in accordance with applicable NARA schedules.

**Section 4.0 Internal Sharing and Disclosure**

The following questions are intended to define the scope of sharing within DHS.

4.1 **With which internal organization(s) is the information shared, what information is shared and for what purpose?**

The benefit application information collected through the e-Filing system is not widely shared with, or used by, other organizations within DHS. Information sharing may occur with other DHS organizations if formally requested for analysis by any of the investigative divisions within USCIS. Specifically, USCIS may provide requested information to Immigration and Customs Enforcement (ICE) to support research into e-Filing system misuse or broader fraudulent activity affecting USCIS.

Once e-Filed data is transferred to CLAIMS3 this data is treated similar to any other CLAIMS3 data and is subject to sharing with other systems, consistent with CLAIMS3 procedures.6

4.2 **How is the information transmitted or disclosed?**

All internal sharing is conducted over a secure and reliable DHS electronic interface or via secure courier. This interface utilizes secure network connections on the DHS core network. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, Safeguarding Personally Identifiable Information, dated May 22, 2006, and M-06-16 Protection of Sensitive Agency Information, dated June 23, 2006, setting forth the standards for the handling and safeguarding of personally

---

6 Please refer to Privacy Act Systems of Record Notice, DHS/USCIS-007, "USCIS Benefits Information System [73 FR 56596 filed September 29, 2008] and the Privacy Impact Assessment for CLAIMS 3 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf)
identifying information. Contractors must also sign non-disclosure agreements.

4.3 **Privacy Impact Analysis:** Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

**Privacy Risk:** The main risk associated with internal information sharing is unauthorized access to the personal information shared.

**Mitigation:** DHS policies and procedures are in place to limit the use of and access to all data in DHS systems to the purposes for which it was collected. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. User access logs track changes to information in the system.

**Privacy Risk:** There is the risk that person(s) without a work-related need to know may gain access to the e-Filing system.

**Mitigation:** In order for internal users to obtain access to the system data, access must be granted through completion of a G-872B form approved by supervisors. All users granted access to the system previously have been cleared for work at USCIS and have been determined to have a need-to-know. Input of a user-ID and password is required for system access. System permissions are role-based and are granted on the principle of “least privilege” which limits the user to only the information required to perform his/her job responsibilities. An audit log is maintained to track all system transactions. Further, computer desktops utilize automatic timeouts and logout of workstations after 20 minutes of inactivity. In addition, there are physical controls, such as inconspicuous placement of computer monitors and workstations, to minimize the likelihood of unauthorized access to sensitive personal information. Designated officials investigate security violations or suspicious activity. The root causes of validated security events are identified and remedial action is taken to avoid repeat events. Access to the e-Filing system servers is restricted to personnel whose job functions require access.

**Section 5.0 External Sharing and Disclosure**

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 **With which external organization(s) is the information shared, what information is shared, and for what purpose?**

USCIS provides payment information to the Department of Treasury’s Pay.gov system for the purposes of processing ACH and credit card payments submitted by the applicant; the e-Filing user submits payment information, as part of the e-Filing submission, through the e-Filing System which then connects to Pay.gov. To the e-Filing user, the application completion and payment submission is a seamless process through the same system. In reality, the e-Filing System collects the payment information, passes it to Pay.gov, and uses the response from Pay.gov (regarding the success of the attempted payment) to
determine the next action necessary with the submission. Pay.gov stores the information consistent with Section 2.1 of this PIA and the e-Filing Privacy Policy.

Also, when third parties, such as law firms and CBOs, assist individuals with the application process, USCIS may release application status information to these parties and grant them access to the e-Filing account.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The current System of Records Notice (SORN) addressing the data collection activities on which the e-Filing system is based is USCIS Benefits Information System, 73 Federal Register (FR) 56596, dated September 29, 2008. All external sharing is covered by an appropriate routine use. All sharing is compatible with the purpose for which the information was originally requested.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The personal payment information is collected and stored in the e-Filing temporary database repository and is electronically routed via an HTTPS post over the Internet (Secure Socket Layer (SSL)) to Pay.gov for processing on a daily basis. Upon processing of the payment information, Pay.gov transmits payment acceptance, rejection, and settlement status data back to the e-Filing system.

The Department of Treasury requires all federal agencies that utilize the services of Pay.gov to complete an Agency Configuration Template (ACT) for each form (e.g., Form I-90 Application to Replace Permanent Resident Card). The ACT reflects the scope of information transmitted between USCIS and the Department of Treasury through the e-Filing system.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: For the e-Filing environment the primary privacy issue in external sharing is the individual may not be aware that USCIS may share submitted information with external entities.

Mitigation: The e-Filing privacy policy advises all e-filers that USCIS may provide information from their application to other government agencies. In order to mitigate the potential risks associated with sharing personal payment information with private sector companies, USCIS chose to instead utilize the Department of Treasury’s Pay.gov services to process e-Filing system payments. The decision to use Pay.gov ensures personal payment information would not be transmitted outside the Federal Government.
With respect to sharing with third parties assisting individuals with the application process, any risk posed is mitigated by the fact that these persons/entities are the appointed/designated representatives of the applicant and thereby authorized to act on the applicant’s behalf.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The USCIS privacy policy is provided to the e-Filing system user on the initial e-Filing system logon page located at https://efiling.uscis.dhs.gov/efile/. The complete statement language is provided in Appendix A.

Individuals are provided general notice though the Benefits Information System (BIS) SORN published in the Federal Register (73 FR 56596). Several rules and notices related to USCIS have also been published in the Federal Register.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Providing information on immigration forms is a voluntary act on the part of the individual seeking a benefit, although receipt of a benefit is preconditioned on receipt of a completed application. Applicants may decline to provide the required information; however, it may result in the denial of the applicant’s benefit request. E-filers may choose to exit the data collection activity, delete completed or partially completed electronic forms or cancel the automated form verification activity prior to their submission. Applicants using e-Filing do not have the right to consent to particular uses of the information after he/she has submitted a benefit application through the e-Filing system.

Although the e-Filing system does collect personal information from applicants, the data collected is used to fulfill the applicant’s request for an immigration benefit. Per the USCIS Privacy Policy statement to e-Filing system customers, “The information provided is used to respond to your message and to help us get you the information you have requested. We only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to any private organizations. The Department of Homeland Security never collects information for commercial marketing.”

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

USCIS benefit applications available through e-Filing require that applicants provide certain
biographic information critical in making an informed adjudication decision to grant or deny a USCIS benefit. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes, including background investigations.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Applicants for USCIS benefits are made aware that the information they are providing is being collected for government purposes. Each immigration form contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants are also advised that the information provided will be shared with other government agencies. Through the USCIS Privacy Notice, individuals are also notified that electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules of the NARA, and in some cases may be covered by the Privacy Act and subject to disclosure under the Freedom of Information Act (FOIA). OMB approved all privacy statements on the forms used to obtained consent.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

When a USCIS customer successfully submits a benefit application via the e-Filing system, a Confirmation Receipt notice and their completed application is automatically generated and provided to the user in electronic format (i.e., Portable Document Format (PDF)). The PDF Confirmation Receipt notice provides, among other data, the applicant’s USCIS Receipt Number and next step instructions on how to complete the processing of their application. The PDF of the completed application contains all the data the customer inputted and submitted during their e-Filing session. The rendered PDF of the application is an exact replica of the OMB-approved version of the benefit application. All e-Filing system customers are encouraged to print and/or save a copy of the PDF Confirmation Receipt notice and Application for their own records.

If a system error occurs during the e-Filing session and the applicant does not receive a PDF copy of their Confirmation Receipt notice or application, they may contact the e-Filing Support Team via email.

---

7 Available at [http://www.uscis.gov/portal/site/uscis](http://www.uscis.gov/portal/site/uscis)
at E-Filing.Support@dhs.gov. The e-Filing Support Team will provide the customer with a copy of their PDF Confirmation Receipt notice via email. Due to security reasons, the e-Filing Support Team cannot provide a copy of the PDF original application via email due to the sensitive nature of the information contained within the document.

Requests for access to records in this system 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 requestor 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 Code of Federal Regulations, Section 5.21), and any other identifying information that may be of assistance in locating the record.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an applicant submits a benefit application and realizes an error has been made, the customer may contact the USCIS National Customer Service Center (NCSC). The NCSC can be reached toll-free at 1 (800) 375-5283 or TTY: 1 (800) 767-1833. The NCSC live assistance is available Monday through Friday as follows:

- Customers calling from Alaska: 8:00 AM to 5:00 PM local time;
- Customers calling from Hawaii: 8:00 AM to 4:00 PM local time;
- Customers calling from Puerto Rico and the U.S. Virgin Islands: 9:00 AM to 6:00 PM local time;
- Customers calling from anywhere else in the United States: 8:00 AM to 6:00 PM local time.
- In Guam, live assistance is available Tuesday through Saturday, 6:00 AM to 11:00 AM local time.
- The best times to call the NCSC for personal assistance are Tuesday through Friday.

In addition to contacting the NCSC, customers using e-Filing may write a letter to the USCIS Service Center responsible for processing their benefit application and request a change to the data on their pending application. If a customer filed a Form I-90 Application to Replace a Permanent Resident Card via the e-Filing system, he/she is instructed to bring physical evidence to support their application change with them to their biometrics capture appointment at the designated USCIS Application Support Center (ASC).

Alternatively, requests to contest or amend information submitted via e-Filing should be made to the system manager or the USCIS FOIA/Privacy Act (PA) officer. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. Clearly mark the envelope, “Privacy Act Amendment Request.” The record must be identified in the same manner as described for making a request for access. Mail requests to: U.S. Citizenship and Immigration Services, National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064-8010.

If the particular USCIS process requires a personal interview, the applicant also has the opportunity
7.3 How are individuals notified of the procedures for correcting their information?

Customers using e-Filing can refer to the official USCIS website (www.uscis.gov) to obtain information regarding changes to their pending benefit applications. For information specifically related to the e-Filing system, the user can refer to the “Introduction to E-Filing” page on the official USCIS website located at http://uscis.gov/graphics/formsfee/forms/eFiling.htm. This page provides detailed guidance on all e-Filing related policies, procedures, and issues.

When published, this notice will provide individuals with guidance regarding the procedures for correcting information. Privacy Act statements, including notice of an individual’s right to correct information, are also contained in most hard copies of immigration forms published by USCIS.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Applicants are provided opportunity for redress as discussed above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The redress and access measures offered by USCIS are appropriate given the purpose of the system. Individuals are given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

In compliance with federal law and regulations, users have access to e-Filing systems on a need to know basis. This need to know is determined by the individual’s current job functions. Users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. Access privileges are established in system tables documenting who has access to what information.
A user desiring access must complete a Form G-872A & B, USCIS and End User Application for access. This application states the justification for the level of access being requested. The requestor’s supervisor, the system owner, and the USCIS Office of the Chief Information Officer (OCIO) review this request; if approved, the requestor’s clearance level is independently confirmed and the user account established.

Criteria, procedures, controls, and responsibilities regarding e-Filing access are contained in the Sensitive System Security plan for e-Filing. Additionally, there are several department and government-wide regulations and directives, which provide additional guidance and direction.

8.2 Will Department contractors have access to the system?

Contractors support portions of the e-Filing environment under the direction of the USCIS Office of Information Technology (OIT). Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant SOPs. In addition, USCIS employees and contractors who have completed a G-872A & B form (see Section 8.4) and granted appropriate access levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All users internal to USCIS must successfully complete the Computer Security Awareness Training (CSAT) annually to be fully compliant with the USCIS Privacy Policy and retain access to systems. The Federal Information Systems Management Act (FISMA) and DHS Policy mandate the CSAT training, which details acceptable computer use. System managers have the responsibility to ensure that all federal employees and contractors receive the required annual computer security awareness training and Privacy Act training.

USCIS customers using the online e-Filing System must register online as a new user before accessing any of the available applications. All new users must acknowledge the Privacy Policy before proceeding with registration, as detailed in the Overview section of this document.

8.4 Has Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

The e-Filing system data is secured in accordance with FISMA requirements. The e-Filing underwent a Certification and Accreditation (C&A) review performed by the USCIS Office of Information Technology (OIT) and was granted an Authority to Operate (ATO). The current ATO will expire in February 2011.
8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

When privileges expire, user access is terminated automatically. Many users have legitimate job duties that require them to query the database for record sets meeting certain criteria. This work is performed under supervisory oversight. Each employee is given annual security awareness training that addresses their duties and responsibilities to protect the data. e-Filing also records History Action Codes that provide a chronology of salient case processing actions including the user ID of the individual performing these actions. Browsing by the general user community is not permitted. In order to reduce the possibility of misuse and inappropriate dissemination of information, DHS security specifications require auditing capabilities that log user activity. All user actions are tracked via audit logs.

E-Filing users are required to follow SOPs. Corresponding audits ensure that local processes and procedures are consistent across the enterprise. Within the application, there are many business rules that ensure data integrity and consistency.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Given the scope of the personal information collected via e-Filing, the security of the information on the system is of critical importance. Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing, including electronic eavesdropping) that require mitigation.

Mitigation: Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Data submission activities via the e-Filing website are protected using the Secure Socket Layer protocol and 1288 bit key encryption. Role-based data access requirements are identified to determine the extent to which an authorized user may access information in the system. Audit trails are kept in order to track and identify any unauthorized changes to information in the system. E-Filing has a comprehensive audit trail tracking and maintenance function that stores information on who submits the query, when the query was run, what the response was, who receives the response, and when the response was received. Data encryption is employed where appropriate to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, e-Filing complies with DHS and FISMA/National Institute for Science and Technology (NIST) security requirements, which provide hardening criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Each time an e-Filing system is modified, the security engineers review the proposed changes and if required, perform an appropriate testing and evaluations to confirm that the controls work properly.
Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, Radio Frequency Identification (RFID), biometrics and other technology.

9.1 What type of project is the program or system?

E-Filing is an on-line information submission system.

9.2 What stage of development is the system in and what project development lifecycle was used?

E-Filing is in the operations and maintenance phase of the DHS system development life cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

E-Filing is an information conduit between e-filers and USCIS related to the application and adjudication of benefits. The system does not include technology or capabilities to monitor the activities of individuals or groups beyond that required to support the submission of application data by the e-filer and the provision of status information by USCIS to the same.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security