



Privacy Impact Assessment
for the

USCIS Electronic Immigration System (USCIS ELIS)

DHS/USCIS/PIA-056

October 30, 2015

Contact Point

Donald Hawkins

Privacy Officer

United States Citizenship and Immigration Services

(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) United States Citizenship and Immigration Services (USCIS) operates the USCIS Electronic Immigration System (USCIS ELIS). USCIS ELIS is an electronic case management system that allows USCIS to process certain immigration benefit requests. USCIS conducted this PIA to evaluate the privacy impacts of converting legacy, paper-based processes to an electronic system. This PIA replaces all previously-issued USCIS ELIS PIAs, which are: DHS/USCIS/PIA-039 *Transformation*, DHS/USCIS/PIA-041 *ELIS-1 Temporary Accounts and Draft Benefit Requests*, DHS/USCIS/PIA-042 *ELIS-2 Account and Case Management*, DHS/USCIS/PIA-043 *ELIS-3 Automated Background Functions*, and DHS-USCIS-PIA-056 *USCIS ELIS: Form I-90*. As USCIS ELIS expands to additional immigration benefit types, USCIS will update the Appendix to this PIA.

Overview

USCIS is the Component within DHS that oversees lawful visits and immigration to the United States. This includes receiving and adjudicating a wide variety of immigration and non-immigration benefits and requests (hereafter referred to as immigration benefits). Historically, USCIS has relied on manual, paper processes to perform this function. USCIS ELIS is a centralized, web-based system designed to transform USCIS business operations from a “transaction-centric” model to a “person-centric” model using unique customer accounts. USCIS is expanding its use of USCIS ELIS over the next several years by expanding the immigration benefit types that USCIS ELIS will process in an incremental fashion. As new immigration benefit types are made available in USCIS ELIS, all benefit requests within that immigration benefit type will be processed in USCIS ELIS, including paper and electronic filings.¹

Background and “Legacy USCIS ELIS”

USCIS ELIS originally launched in the spring of 2012. USCIS is conducting this PIA to describe a new iteration of the existing USCIS ELIS system. The current USCIS ELIS system, now known as the “Legacy USCIS ELIS” system, is no longer accepting documents and will be decommissioned. The two systems are completely separate, including separate login accounts for customers and employees and a different user interface. However, the new system does follow the same general purpose and data collection process as the previously-used system. Each system accepts different immigration benefit types,² which limits the number of customers who have reason to access both systems.

¹ Except for certain low-volume special circumstances that will not be processed in ELIS.

² Legacy USCIS ELIS processed the electronic Form I-539, Application to Extend Stay/Change Status as a Nonimmigrant; electronic Form I-526, Immigrant Petition by Alien Entrepreneur; a Document Library (for EB-5 petitions associated with Regional Centers); and the ability to pay the \$165 USCIS Immigrant Fee.



The primary users of USCIS ELIS are USCIS adjudicators processing benefit requests. USCIS ELIS also interfaces with other IT systems that conduct other functions, such as customer service and fraud detection, without subsuming or replacing those functions. Unlike Legacy USCIS ELIS, USCIS ELIS does not attempt to conduct advanced link-analysis for fraud or national security purposes.³ Instead, it interfaces directly with other USCIS systems that are operated specifically for those purposes. Therefore, with the publication of this PIA, USCIS is retiring the previous USCIS ELIS PIAs.

System Description

Paper Intake

Historically, USCIS has required applicants, petitioners, or benefit requestors submit hard-copy, paper submissions of immigration applications, petitions, or benefit requests to one of its “Lockbox” facilities. Lockbox facilities are operated by U.S. Department of Treasury financial agents on behalf of USCIS to receive paper requests, process payments, and forward the requests to USCIS Service Centers in paper and electronic format for further processing. As USCIS ELIS expands to new immigration benefit types, the applicable Lockbox facility will adjust its legacy delivery process to transmit filings to USCIS ELIS rather than to the legacy system (usually CLAIMS 3 or CLAIMS 4). It will transmit the data to USCIS ELIS as well as scanned images of the paper filings to ELIS electronic storage.

The Lockbox will continue to follow existing USCIS guidance to prepare submitted paper filings. If the paper filing pertains to an individual with a paper Alien File (A-File),⁴ then the paper will be delivered to that file. If it pertains to a customer without a paper A-File (primarily nonimmigrants), then the paper will be transferred to a Receipt File and delivered to the relevant USCIS office for temporary retention. This temporary retention is governed by the applicable National Archives and Records Administration (NARA)-approved retention schedule. As USCIS expands its use of electronic records, USCIS intends to reduce its storage of paper records when NARA-approved electronic equivalents exist. All changes to retention of records are coordinated with NARA, published in the *Federal Register*, and communicated to the USCIS customer in the instructions of each immigration form.

Once information from the paper filing is accepted in USCIS ELIS, the system sends the customer a “USCIS Account Acceptance Notice” via U.S. Postal Service mail. This notice contains instructions for creating a USCIS Online Account and a passcode for linking the account with the USCIS ELIS case. If the customer opts not to activate his or her USCIS Online Account, the passcode expires in 30 days as a security measure. The customer, however, may later contact USCIS customer service to request that a new letter with a new activation passcode be sent. Customers who file paper applications, petitions, or requests that are received into USCIS ELIS

³ DHS/USCIS/PIA-043, *ELIS-3 Automated Background Functions* (May 16, 2012), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_elis_3_automatedbackgroundfunctions.pdf.

⁴ 78 FR 69864 (Nov. 21, 2013).



will have the opportunity to log in to their USCIS ELIS account to check the status of their application, petition, or request; obtain copies of documents associated with the filing; and respond electronically to requests for additional information, such as Requests for Evidence (RFEs), if they create online accounts. Customers who opt not to activate their online accounts can continue to use the existing paper process and USCIS will continue to send notices via hard copy mail.

Electronic Intake

Customers may also file benefit requests with USCIS electronically. Customers who choose to file electronically must first create a USCIS Online Account by providing a person-specific, unique email address. USCIS sends a confirmation email to the provided address to confirm accuracy. The email address is then stored as the customer's username. Next, the customer creates a strong password. To establish two-factor authentication, a personal identification number (PIN) is required in addition to the password. The customer must choose whether to receive the one-time PIN either by mobile phone via short message service (SMS), or as a message delivered by email. If the customer chooses SMS, the system prompts him or her to provide the mobile number and carrier. Passwords are never sent or reset via email.

The customer also provides answers to security questions that he or she will answer to reset the account password in the future. The security questions are "fill-in-the-blank" questions that the customer provides the answer to at account set-up. USCIS provides the customer with a drop-down menu of standard questions, and the customer chooses which ones to use as his or her security questions.⁵ USCIS will not use the answers to these questions for purposes other than assisting with password resets (e.g., the answers would not be available to adjudicators for an immigration benefit purpose or fraud investigators in the event of a fraud investigation). These answers are stored by USCIS within the system, but like passwords, are not visible however via the user interface used by USCIS adjudicators, clerks, and similar users. The answers could be visible to customer helpdesk personnel who assist users in resetting their passwords and encountering problems using the system.

Once the online account is set-up, the customer can begin drafting his or her electronic request in the online filing system. The user interface collects the same information as is collected via the corresponding existing paper form, although questions dynamically expand or become disabled as the customer progresses through the request. In other words, a customer's answer to one question may prevent a series of additional questions from being necessary. Those would not be fillable because they would not be applicable to that customer. This enables the customer to respond only to applicable questions. Although USCIS ELIS initially saves draft data; the customer may edit, delete, or update information when it is in draft state and the system does not keep copies of these previous iterations.

⁵ For example, the applicant may choose, *What is your favorite type of candy?* as a security question.



The electronic format also provides some advantages to the user, such as a validation of mailing address against U.S. Postal Service (USPS) known addresses. The user has the option to use a corrected address, validated by the USPS Address Standardization Web Tool,⁶ to prevent address formatting confusion or typographical errors. When the customer enters his or her mailing address, the system bounces the address entered against addresses recognized by USPS. If the USPS tool does not recognize the address, the system will display a pop-up window informing the customer that the address was not found. The pop-up window will also offer an alternative recognized address that the USPS tool provides as a close match. If there is no close match, the USPS tool provides an alternative address as a suggestion. The customer is given the option to accept the suggested address or ignore the suggestion and use the address he or she originally typed. The customer may return to the address fields at any time, which will trigger a re-validation by the USPS service.

Based on the answers the customer provides, ELIS prompts the customer to upload evidence. For example, if the customer requests a replacement Permanent Resident Card because of a legal name change through marriage, the system will prompt the customer to upload evidence of the legal name change, such as a marriage certificate. Customers upload evidence by scanning documents and attaching the scanned images to the USCIS ELIS electronic request.

Once the customer completes the request and uploads necessary evidence, USCIS ELIS requires the customer to electronically sign (e-sign) the request and pay the applicable fee. The customer can review the information he or she is about to submit, and then e-sign by entering his or her name. Payment is made using the U.S. Department of Treasury's Pay.Gov service.⁷ USCIS does not collect the fee directly. Rather, the Pay.Gov interface is imbedded within the USCIS Online Account user interface, and Pay.Gov collects payment information—either credit card, debit card, or Automated Clearing House (ACH) debit from a personal bank account. Once Pay.Gov validates the payment information, applicants are routed back to USCIS ELIS and the USCIS Online Account confirms to the customer that he or she successfully submitted the request. USCIS will mail a receipt notice (if applicable) to the customer's physical address and make it available electronically via a new interface called the USCIS Online Account.

Intake with Attorney or Accredited Representative

Attorneys and non-attorney representatives accredited by the Board of Immigration Appeals (BIA) (hereafter referred to as Representatives) may also create a USCIS Online Account to use USCIS ELIS. These accounts require limited biographic data about the Representative (based on the USCIS Form G-28, *Notice of Appearance as Attorney or Accredited Representative*) and allow the Representative to draft electronic requests on behalf of his or her clients;

⁶ Via this service, USPS does not ingest or store the address provided by USCIS ELIS.

⁷ U.S. Department of Treasury *Financial Management Services Pay.Gov Privacy Impact Assessment 2.0* (July 1, 2011), available at, http://fms.treas.gov/pia/paygov_pia%20.pdf.



electronically transfer draft requests for client review and e-signature; and receive updates about those requests as they are processed by USCIS.

Customers give a Representative permission to represent them on a particular request via Form G-28, *Notice of Entry of Appearance as Attorney or Accredited Representative*, filed concurrently with that request. If a paper filing for a USCIS ELIS immigration benefit type is submitted with a Form G-28, the Lockbox will transmit the information to USCIS ELIS, which will search to identify whether that Representative already has a USCIS Representative account in the system. If a Representative account already exists, the new filing is linked to the existing account. However, if a Representative account does not yet exist, USCIS ELIS will create a USCIS Online Account for the Representative. Like customers, Representatives are sent a hardcopy “USCIS Account Acceptance Notice” via USPS. This letter contains instructions on activating the account as well as a passcode for linking the new account with the client immigration request in USCIS ELIS.

Representatives may also electronically file requests in USCIS ELIS. To successfully submit a represented filing in USCIS ELIS, both the Representative and the Representative’s client (who is the USCIS customer) must have their own, independent USCIS Online Account. The Representative uses his or her account to draft a request for his or her client, and upon completion, submits it for the client’s review. When the Representative submits the draft benefit request for client review, the Representative provides USCIS ELIS with the client’s email address. USCIS ELIS then presents the Representative with a passcode that is provided in-person to his or her client. The client must provide the passcode in order to access to the draft request when he or she next logs in to the system. USCIS ELIS sends the client an email indicating the pending draft in his or her existing account, and upon login, the customer is directed to input the passcode in order to view the draft. USCIS ELIS gives the client access to the draft case filed by the Representative if both the email address connected to the client’s account and the passcode entered by the client match the client email address and the passcode associated with the filing submitted via the Representative’s account. The client has read-only access to the Representative’s draft. The client is able to reject the draft, which sends it back to the Representative, or accept the draft and e-sign it together with the electronic Form G-28. If the client rejects the draft, the Representative may overwrite the previous draft. The customer, however, will need a new passcode in order to access the revised document. USCIS ELIS does not store previous drafts. Once the client reviews the request, he or she accepts and e-signs. It is then electronically returned to the Representative, who will also e-sign, pay filing fees, and submit the request to USCIS. Thereafter, the Representative will have access to the same request information and status updates related to the request that the client does.

Remote Identity Proofing

USCIS requires in-person identity verification for many of its immigration benefits, either by requiring customers to appear in-person to submit biometrics, to be interviewed in-person by



an adjudicator, or both. However, there will be some USCIS Online Account holders who never appear in-person, and require remote identity proofing to assure USCIS that the account holder is who he or she purports to be. Those requiring remote identity proofing include customers making requests that do not include in-person appearances for adjudication, and also other users such as Representatives, who do not appear in person.

USCIS will provide remote identity proofing for those users who require it using two methods. The first method will use a third-party remote identity proofing service that uses an individual's commercial and financial data to verify identity using an "out of wallet" quiz. These services are standard across public and private sector online interfaces and are designed to conform to applicable Government-wide standards on identity proofing of federal systems. USCIS ELIS will use those services as described in the DHS E-Authentication System of Records Notice.⁸

Those existing services, however, are largely unable to identity-proof individuals who have not lived or conducted business in the United States, which is a large portion of USCIS customers. For those customers, USCIS has designed Identity Proofing as a Service (IDPaaS.) IDPaaS will use data on file within USCIS legacy systems or data collected by the Department of State abroad to verify that the USCIS Online Account holder is the customer he or she claims to be. IDPaaS will present a quiz to the account-holder based on the data in a fashion similar to commercial "out-of-wallet" quizzes.

The questions presented to each account-holder are dynamically generated based on the best information USCIS has about the individual, as well as the most diverse set of questions available. This data originally comes from information the Department of State collected in-person when issuing a visa, information U.S. Custom and Border Protection (CBP) collects in-person upon entry at the border, and information USCIS has from the customer based on previous immigration benefit requests, as consolidated by USCIS in its major immigration systems.⁹ In designing the questionnaire, USCIS looked at the breadth of data and categorized it into several domains based on the type of information, such as travel, contact information, etc. The questionnaire is designed to dynamically ask the customer questions from different domains to ensure the customer is showing knowledge of a wide breadth of data about him- or herself, and also data that would not be known by a different person. IDPaaS may allow customers more than one attempt to pass the questionnaire, but only if the system has enough reliable data in enough domains about that individual. Questions are in multiple-choice format, and include a "none of the above" option where appropriate.

Customers who are required to use IDPaaS are provided notice explaining what identity proofing is and what to expect before launching into the process. If customers are unable to pass the IDPaaS questionnaire, they are presented with instructions on how to proceed, which may be by contacting Customer Service or appearing in-person. Once the customer passes the identity

⁸ DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (Aug. 11, 2014).

⁹ 78 FR 20673 (Apr. 5, 2013), 78 FR 69864 (Nov. 21, 2013).



proofing quiz, USCIS ELIS retains the fact that the customer has been identity-proofed and does not require the customer to repeat the process for subsequent immigration benefit requests.

As IDPaaS is incrementally deployed, USCIS will maintain an internal governance board¹⁰ to review the efficacy of the system, approve new questions and methods of verifying identity, and evolve the questionnaires as appropriate for each new use case. IDPaaS will only be used internally within USCIS. Data from sources will be shared as it resides in other systems.

System Process

Automated System Checks

Upon receipt of a request, the first data element USCIS ELIS validates is the customer's Alien Registration Number (A-Number), if applicable. When customers list an A-Number on a benefit request, USCIS ELIS runs an automated comparison of the claimed A-Number against the USCIS legacy Central Index System (CIS)¹¹ to verify that: the A-Number exists and is valid and matches the name and identifying information provided by the customer. If the system cannot automatically verify this information, USCIS ELIS moves the customer's request into an electronic work queue where it will be researched and resolved by a USCIS employee or contractor before proceeding to adjudication.

During the A-Number validation, USCIS also runs a criminal and national security background check against the CBP TECS system.¹² If this check identifies potential criminal or national security issues, it is referred to another electronic workflow queue for resolution. USCIS must take measures to address or resolve the presented issues before adjudicating the benefit request, which may include a referral to the USCIS Fraud Detection and National Security (FDNS) Directorate.

After the A-Number is validated, USCIS ELIS interfaces with the National Appointment Scheduling Service (NASS)¹³ to schedule an Application Support Center (ASC) appointment for the customer if required for the particular request. During an ASC appointment, USCIS is able to verify identity in-person by collecting biometrics. NASS generates an appointment notice that USCIS mails to the customer. USCIS ELIS holds the customer's request pending completion of the ASC appointment, if required.

¹⁰ Members include designees from USCIS Office of Privacy, Office of Chief Counsel, and Office of the Chief Information Security Officer, among others.

¹¹ DHS/USCIS/PIA-009, Central Index System PIA (June 22, 2007), *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf.

¹² DHS/CBP/PIA-009, TECS System: CBP Primary and Secondary Processing PIA (December 22, 2010), *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_tecs.pdf.

¹³ Privacy Impact Assessment pending publication to <http://www.dhs.gov/uscis-pias-and-sorns>.



Adjudicating the Application

The customer's case advances once the USCIS Customer Profile Management System (CPMS)¹⁴ sends notification that the customer has submitted his or her biometrics at the ASC, if required. If biometrics are not required, the case advances to the adjudication step immediately following A-Number validation and resolution of any background check results.

USCIS ELIS automatically places the application in an adjudicator work queue after A-Number validation, completion of the TECS background check, and return of the background and security check results through the legacy USCIS Benefits Biometric Support System (BBSS)¹⁵ have occurred. The USCIS adjudicator evaluates all data—the information submitted by the customer along with the results of the background and security checks—according to existing standard operating procedures (SOP) that apply to the legacy paper process.

To assist the adjudicator in verifying information submitted by the customer, ELIS aggregates and displays information pulled from other USCIS systems via the Person-Centric Query System (PCQS).¹⁶ This information includes other names, dates of birth, contact information, and other A-Numbers that may also be associated with the customer. Following existing SOPs, the adjudicator is able to identify which data is correct or relevant, and make updates to the system to record the correct data about a customer. The system documents all updates made to data about the customer. The adjudicator then renders a decision, and may electronically submit the decision to his or her supervisor for review.

Once the decision is final, USCIS ELIS uses automated interfaces with existing USCIS IT systems to send approval or denial notices along with the proof of benefit (such as a Lawful Permanent Resident card), as applicable. When a proof of benefit must be produced, and it requires a photograph, the adjudicator is able to obtain the customer's facial photograph, fingerprint, and signature via an interface with CPMS solely for proof of benefit production purposes. The facial photograph and other biometric elements are temporarily displayed in USCIS ELIS and can be adjusted to improve image quality for printing. USCIS ELIS allows the user to zoom, pan, lighten, or darken the photo for card production, and then certify for printing. Upon successful card printing, the facial photograph is automatically deleted from USCIS ELIS and the final adjusted image is stored as part of the printed card record in CPMS.

System Privacy Impacts

Overall, USCIS ELIS offers USCIS customers several advantages with respect to data privacy protections. Once logged into their account, USCIS customers are able to enter their information directly into the system or correct data as applicable. In contrast, the paper-based

¹⁴ *Id.*

¹⁵ DHS/USCIS/PIA-033 Immigration Benefit Background Check System PIA (November 5, 2010) *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_ibbcs.pdf.

¹⁶ DHS/USCIS/PIA-010 Person-Centric Query System (PCQS) PIA (June 22, 2007), *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_pcq.pdf.



legacy process requires contractors to manually key-in data from paper filings. Allowing customers to enter or correct their information directly reduces the risk for typographical errors and generally improves the accuracy, timeliness, and completeness of submitted information. USCIS ELIS customers who have activated their USCIS Online Accounts also enjoy improved transparency regarding the status of their requests and better access to their data, because that data is available instantly once they are logged into their account. Although USCIS ELIS initially saves draft data; the customer may edit, delete, or update information when it is in draft state and the system does not keep copies of these previous iterations. This preserves the same confidentiality for an electronic customer as a paper-filer. IDPaaS allows USCIS ELIS to ensure many customers online are who they claim to be. There is a risk that some legitimate customers may be unable to pass the IDPaaS quiz, and there is a risk that an individual with access to a customer's files could illegitimately pass. USCIS will actively mitigate this risk by monitoring the performance of the system and assisting with customer help requests, and adjust for needed changes accordingly. Customers with online accounts also may receive requests for additional information and other communications more quickly, as information and notices are made available electronically in the account. This method of communication is faster than sending customers paper notices via USPS mail. While faster, use of email and the internet creates other risks. Customers may face some increased data security risk by virtue of submitting data via the Internet. To mitigate this risk, USCIS ELIS employs several layered IT security and data quality measures, such as establishing a secure encrypted connection when a customer is entering sensitive personally identifiable information (PII) and requiring strong two-factor authentication.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The primary legal authority supporting the collection of the information provided to USCIS is 8 U.S.C. § 1101 *et seq.* Specifically, 8 U.S.C. § 1360 requires a central file of information for the security and enforcement agencies of the Government of the United States that contains the names of all aliens admitted or denied admission to the United States and such other relevant information as required to aid in the proper enforcement of this chapter. The Homeland Security Act of 2002¹⁷ and the Immigration Nationality Act (INA)¹⁸ charge the Secretary of Homeland Security with administration and enforcement of the immigration and naturalization laws. The Secretary of Homeland Security has delegated duties to USCIS pursuant to DHS Management Directive MD 0150.1. DHS also has promulgated regulations that permit the collection and

¹⁷ Pub. L. No.107-296, 116 Stat. 2135 (2002), 6 U.S.C. § 112.

¹⁸ 8 U.S.C. § 1101 (2004) *et seq.*



processing of applications, petitions, and requests online entitled, “Immigration Benefits Business Transformation, Increment I,¹⁹” and “Immigration Benefits Business Transformation, Increment I; Correction.²⁰”

The Government Paperwork Elimination Act (GPEA)²¹ provides that, when possible, federal agencies should use electronic forms, electronic filing, and electronic submissions to conduct agency business with the public. GPEA establishes the criteria and guidelines for the use of electronic signatures. Executive Order 13571²² requires federal agencies to develop plans to streamline delivery of services and improve customer service by exploring lower-cost, self-service options accessed by the Internet or mobile phone, and improved processes that deliver services faster and more responsively, reducing the overall need for customer inquiries and complaints.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs cover USCIS ELIS:

- DHS/USCIS-007 Benefits Information System;²³
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,²⁴ and
- DHS/ALL-037 E-Authentication Records System of Records.²⁵

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. USCIS ELIS has been granted an Authority to Operate (ATO), which is continually being monitored under the USCIS Ongoing Authorization process. USCIS ELIS data also includes data from the USCIS Identity and Credentialing Account Management system (ICAM) and the USCIS Online Account system, also under USCIS Ongoing Authorization.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes: N1-566-11-02, (October 17, 2011) and N1-566-12-05, (April 17, 2013) cover USCIS ELIS accounts. Each immigration benefit type processed by USCIS ELIS has an additional existing retention schedule, which USCIS ELIS applies to each particular case.

¹⁹ 76 FR 53764 (Aug. 29, 2011).

²⁰ 76 FR 73475, (Nov. 29, 2011).

²¹ 44 U.S.C. § 3504 (2004).

²² 75 FR 24339 (Apr. 27, 2011).

²³ 78 FR 20673 (Apr. 5, 2013).

²⁴ 78 FR 69864 (Nov. 21, 2013).

²⁵ 73 FR 56596 (Sept. 29, 2008).



1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The OMB Control number for online account setup is 1615-0122 (there is no corresponding agency number.) Each form processed by USCIS ELIS has an existing OMB control number that covers the USCIS ELIS collection. An updated list is available in Appendix A of this document.

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

USCIS ELIS collects:

- Account setup and login information including: email address, password, security questions, mobile phone number, and mobile phone carrier;
- Information that is required to adjudicate the request: This will vary for each immigration benefit type. A full account of what data is requested for each immigration benefit type can be viewed by referencing the paper forms associated with each immigration benefit type in Appendix A;
- E-signature: check-box attestation, the customer's name, Internet Protocol (IP) address from which the filing is submitted, and time/date stamp;
- Background and security check information about the customer as described below, whether the result relates to the individual, and if applicable, memoranda from adjudicators resolving the results; and
- Temporarily stores biometric images to allow proper formatting for printing.

2.2 What are the sources of the information and how is the information collected for the project?

The majority of information in USCIS ELIS is obtained directly from the customer or his or her Representative. Additionally, USCIS collects data from CBP TECS and USCIS BBSS in order to conduct background and security checks. USCIS ELIS also receives information from the



Department of State (DoS) Consolidated Consular Database (CCD)²⁶ for Immigrant Visa data when applicable. CCD data is transmitted via PCQS and its data is necessary for USCIS because CCD contains immigrant and non-immigrant visa data. USCIS employees and contractors using the system may generate data, such as notices, internal case processing notes, and decisions.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

USCIS ELIS ensures data accuracy because the system uses data entered directly by the individual customers whenever possible. Requests filed using the USCIS Online Accounts are completed directly by the individual customers. Customers are able to overwrite and correct any information in their applications up to the point that they sign and submit the application. After it has been submitted, the customer may login to his or her account and automatically make changes that have no substantive bearing on the adjudication, such as updating an email address or other contact information. When inputting data from a paper filing, the Lockbox facilities employ quality control measures, including levels of review to prevent keying errors. In the event of an error, the customer is able to correct certain data using existing legacy correction processes, such as contacting USCIS Customer Service.

Select data submitted by the individual customers are run through the A-Number validation process to promote data integrity between USCIS ELIS and legacy USCIS systems such as the Central Index System (CIS). USCIS ELIS also enables the adjudicator to check biographical data entered by the customer (e.g., name, date of birth, place of birth, gender) against data from CIS to assist the adjudicator in identifying inaccurate data supplied by the customer (or correct inaccurate data on file in legacy systems.) Finally, USCIS automatically submits data to other federal systems such as CBP TECS and USCIS BBSS to verify identity and conduct background and security checks.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Because USCIS ELIS houses multiple benefit requests that each require different information, there is a risk that customers could submit more information than necessary.

Mitigation: USCIS ELIS mitigates this risk in two main ways. First, the system only collects information pertaining to one request at a time, so that the customer cannot be prompted

²⁶ Department of State Consolidated Consular Database Privacy Impact Assessment (Dec. 11, 2008), *available at* <http://www.state.gov/documents/organizaition/93772.pdf>.



to enter information unless it pertains to the specific benefit request on which the customer is working. Second, the user interface dynamically greys out fields that the customer should not fill out based on answers to other questions. For example, when a paper form would instruct the customer to skip a section of the form based on her answer, USCIS ELIS would “grey out” or disable the inapplicable section and present the customer only relevant sections and questions. It is possible for customers to upload more evidence than necessary because they are allowed to submit “unsolicited evidence” at any point until adjudication. This is a valuable feature to allow customers the opportunity to provide information initially forgotten or submitted incorrectly, which partially mitigates the risk that customers may opt to provide too much information. This risk cannot be fully mitigated because of the “unsolicited evidence” option.

Privacy Risk: Because USCIS ELIS automatically saves draft applications, there is a risk that adjudicators could later see draft information that the customer deleted or corrected before submitting his or her electronic request. This could negatively affect USCIS ELIS customers because they would not receive the same confidentiality online they receive via the paper process.

Mitigation: Although USCIS ELIS initially saves draft data; the customer may edit, delete, or update information when it is in draft state and the system does not keep copies of these previous iterations. When the customer submits his or her electronic request, USCIS ELIS only stores the final, signed version. Any previous version, including uploaded evidence that the customer removed before finalizing, is permanently deleted. USCIS adjudicators only receive the information that was e-signed and submitted. Similarly, if the customer begins drafting a request but never submits it (by e-signing and paying), then USCIS ELIS automatically deletes the data after 30 days, per the approved retention schedule. If the customer later files another benefit request, the adjudicator has no indication of a previous draft.

Section 3.0 Uses of the Information

The following questions require a clear description of the project’s use of information.

3.1 Describe how and why the project uses the information.

USCIS collects only the minimum information necessary to fulfill the following purposes:

(1) Establish a secure online account through which to submit an application

Information collected includes email address (used to contact customer and also as username), password (used to authenticate the user), mobile phone number for sending one-time PIN to be used as a second-factor in authenticating, and answers to security questions for future password resets;



(2) Verify the identity of the requester

Information collected may include A-Number, name, date of birth, place of birth, Social Security number, and other information such as date and class of admission into the United States, and mother's and father's names. These data are used to locate the customer in legacy systems;

(3) Facilitate criminal and national security background checks

Information collected includes name, date of birth, and country of birth for use by CBP TECS and USCIS BBSS in running background checks; physical description (eye color, hair color, height, and weight) required by BBSS; mailing address to provide to USCIS NASS for biometric appointment scheduling; and results of criminal and national security background checks from CBP TECS and USCIS BBSS for referral to FDNS as needed;

(4) Justify eligibility for benefit requested

Information collected includes the information collected on the applicable request along with documentation to support the request. The adjudicator uses all of this to follow existing SOPs on adjudicating the particular request; and

(5) Authorize card production

Information collected includes internal system indicators that record that every step of the adjudication process was followed, the adjudicator's decision and supervisory review, and the temporary storage of the applicable biometric images to allow for proper formatting. This also includes information from Pay.gov confirming that the customer paid the applicable fee and e-signature information to record that the customer attests that the information he or she put forth in the application is true.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

USCIS ELIS allows read-only roles for Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), both within DHS because of their shared immigration missions. Also, USCIS ELIS does share read-only information with the USCIS Enterprise Service Bus (ESB),²⁷ which may share information from USCIS ELIS with other Components via PCQS.

²⁷ DHS/USCIS/PIA-010 Person-Centric Query System (PCQS) PIA (June 22, 2007), available at, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_pcq.pdf.



The majority of PCQS users are internal to USCIS. However, PCQS does grant user access to Department of State (DoS) users who have an official need for read-only access to USCIS customer data. Like CBP and ICE, DoS has a shared mission with USCIS because of its visa-issuing authority, which is part of the immigration process for many USCIS customers.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that increased availability of information that previously was only visible to one employee at a time (because it was in a paper file) could result in new, unauthorized uses of the information.

Mitigation: This risk is partially mitigated. USCIS will mitigate this risk three ways. First, all users of USCIS ELIS must receive role-based system training, which explains the purpose of the data and includes reminders about proper PII handling. Second, the system tracks all access and edits to customer PII, and stores that activity in back-end audit logs available to the USCIS Office of Security Investigations (OSI) for monitoring and action. Finally, USCIS ELIS employs a provisioning process that verifies every user requesting access to the system has a valid need to view data in the system.

Privacy Risk: By retaining data in an active, online platform, USCIS ELIS poses a risk of unauthorized exposure because the system could be attacked by an external entity.

Mitigation: USCIS recognizes that retaining data online makes that data potentially more available to compromise. As a result, USCIS is building into its retention schedules a timeframe after which data may be retained offline by the agency but not available online with public access. This will allow the agency to preserve records that should be maintained for their historical value but adds some security from unauthorized access of outdated accounts. This risk is also mitigated by IT security measures such as encryption of the data in transit and at risk and requiring secure, two-factor authentication for login.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

USCIS provides online customers with a Privacy Act statement addressing the collection of their information for the creation of an online account before any information is input by the customer. USCIS also provides a Privacy Act statement covering the particular application, petition, or request at the time of that collection. USCIS ELIS additionally sends paper and



electronic notices pertaining to the customer's request throughout the adjudication process and via this PIA. Further, USCIS provides the appropriate OMB control number and Paperwork Reduction Act Statement for each individual form type available to a customer via the USCIS Online Account prior to any data being input by the customer.

Finally, customers who are required to use IDPaaS are provided notice explaining what identity proofing is and what to expect before launching into the process. If customers are unable to pass the IDPaaS questionnaire, they are presented with instructions on how to proceed, which may be by contacting Customer Service or appearing in-person.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Once USCIS ELIS incorporates a particular immigration benefit type, all requests received for that benefit type will be processed in USCIS ELIS. While customers cannot opt to have their request processed according to a legacy process or system, they may opt to file via paper rather than electronically. If the customer opts not to provide answers to some of the information requested, the system will generally allow the customer to proceed with the request. The request, however, may take longer to adjudicate because the adjudicator may need to request the information the customer declined to submit with his or her application. If the customer declines to provide the requested information, the adjudicator may consider the request to be abandoned and deny the request or consider it abandoned.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that someone other than the USCIS customer will use the system to fraudulently obtain an immigration benefit, which could expose the legitimate customer to identity theft. This could occur without the customer knowing.

Mitigation: In order to mitigate the risk of identity theft or fraud, USCIS has existing processes that require most customers requesting an immigration benefit to provide their biometrics at an ASC, which allows for in-person identity verification. USCIS ELIS leverages this in-person identity-proofing to ensure the individual who created the online account is who he or she claims to be. For those processes that do not include an in-person identity verification, USCIS directs users to a remote identity proofing solution to confirm the user's identity according to applicable government-wide standards.



Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

USCIS has drafted a series of retention schedules to cover different types of data in USCIS ELIS. Currently, two of those schedules have been finalized and signed by the Archivist. The remaining schedules are being actively worked with NARA.

The majority of customer data in USCIS ELIS is not yet covered by a finalized retention schedule, but is pending review at the National Archives. USCIS expects NARA to approve permanent retention for USCIS ELIS customer data because it replaces data that would have been in the Alien File (A-file) if filed via paper. Data includes individual customer account data of immigrants, as well as the case data pertaining to their requests. The A-file is permanently retained for historical purposes.

The approved retention schedules are as follows:

- 1. ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS) ABANDONED DRAFT ACCOUNT AND/OR DRAFT BENEFIT REQUEST DATA, N1-566-11-02, (October 17, 2011):** This schedule covers customer accounts and draft applications that customers do not submit to USCIS within a 30-day period. The schedule dictates that the data must be permanently deleted 30 days after creation of the account or initiation of a draft application.
- 2. USCIS ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS) TEMPORARY ACCOUNTS, N1-566-12-05, (April 17, 2013):** Covers internal user accounts for USCIS employees; such accounts will be deleted/destroyed 6 years after the account is terminated or when no longer needed for investigative or security purposes, whichever is later.

5.2 Privacy Impact Analysis: Related to Retention

There is no privacy risk to retention because USCIS records are retained permanently for their historical value, such as genealogical research, similar to the A-File.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local governments, and private sector entities.

- 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the**



information is accessed and how it is to be used.

USCIS ELIS information is shared outside of USCIS in a read-only state over the ESB and may be viewable by DoS via PCQS. Also, USCIS ELIS feeds data to USCIS BBSS for background checks, and BBSS uses that data as part of the record that is forwarded to the Federal Bureau of Investigations (FBI) to conduct its criminal and national security checks.²⁸

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing USCIS ELIS data via PCQS to DoS is compatible with the purpose of the system because the DoS mission, like USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. This sharing is covered by the Routine Use “I” of the DHS/USCIS-007 SORN,²⁹ which states that data may be shared with, “...the Department of State for the purpose of assisting in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.” Sharing with the FBI is covered by Routine Use “J” of the DHS/USCIS-007 SORN,³⁰ which states that data may be shared with “...appropriate Federal... law enforcement... agencies... during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates to elicit information required by DHS to carry out its functions and statutory mandates.”

6.3 Does the project place limitations on re-dissemination?

USCIS ELIS does not share any data that would not be allowed to be re-disseminated, and does allow for re-dissemination of information only once it becomes part of the sharing partners’ systems of records.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

BBSS and PCQS each automatically log external disclosures of information, as described in those systems’ respective PIAs.³¹ If external sharing is authorized, the USCIS employee who disclosed the information must record the disclosure. The employee records this by typing a note with the data shared, purpose, and date into the free-text comment field of the system.

²⁸ All DHS PIAs and SORNs are available on www.dhs.gov/privacy. Please consult the PCQS and Background Check Service SORNs for specific information about when information is shared, for what purposes, and with whom.

²⁹ 73 FR 56596

³⁰ *Id.*

³¹ All DHS PIAs and SORNs are available on www.dhs.gov/privacy. Please consult the PCQS and BCS PIAs for specific information about how external disclosures are recorded.



6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data-sharing governance and record keeping designed for legacy paper processes, such as paper mechanisms for logging records of disclosure and physical restrictions on paper file sharing, might not translate to the electronic environment.

Mitigation: USCIS is mitigating this risk by working cooperatively with NARA and its records office to address recordkeeping changes as new benefit types are incorporated into the system. Updates are regularly briefed out to the highest level of the USCIS ELIS governance boards, which include USCIS Privacy. To date, recordkeeping issues have not arisen but a continuous review process continues. As the system is expanded to cover a larger percentage of overall customers, USCIS will increase data sharing incrementally so that processes for governance and recordkeeping can be adjusted on a specific basis and documented more formally. Significant updates will be referenced as appropriate in either an updated PIA or an appendix to this PIA.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

USCIS ELIS provides USCIS customers the opportunity to access their information online by logging in to their account. The information they access includes a copy of the application they submitted, any notices or notifications generated by USCIS, and information about the status of their application. Certain information generated by USCIS as part of a criminal or security check is not automatically accessible by the customer. This information is exempt from access under 5 U.S.C. § 552a(k)(2) of the Privacy Act.³²

An individual may also gain access to his or her USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record the request can be mailed to the following address:

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

³² 76 FR 70638 (Nov. 15, 2011).



The information requested may, however, be exempt from access under the Privacy Act because records related to fraud, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations. Further information for Privacy Act and FOIA requests for USCIS records can also be found at <http://www.uscis.gov>.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

USCIS ELIS allows a customer to overwrite and correct any information in his or her application up to the point that he or she e-signs and submits the application. After it has been submitted, the customer may log in to his or her account and automatically make changes that have no substantive bearing on the adjudication, such as change in email address or contact information. If the customer wants to correct inaccurate information while the benefit is being adjudicated, he or she may submit the request in writing and upload the request into USCIS ELIS as unsolicited evidence or by mail. It is the adjudicator's decision to incorporate that corrected information, depending on the timing and validity of the information. For corrections after the application has been adjudicated, the customer would use the existing correction processes employed by USCIS, depending on the type and context of the correction requested.

7.3 How does the project notify individuals about the procedures for correcting their information?

USCIS ELIS makes multiple notifications to the customer throughout his or her use of the system, indicating to the customer when the case is in draft, how to update contact information, and several other methods of correction. Additionally, USCIS ELIS will publish online Frequently Asked Questions that address when and how to make corrections. Finally, USCIS has a Customer Contact Center contact listed to which customers are directed if they have questions. Customers who fail to identity proof using IDPaaS will be given specific instructions on how to proceed, which may be by contacting Customer Service or appearing in-person.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the customer may be unable to correct certain data, such as name and date of birth, after the application is submitted.

Mitigation: Making changes to certain essential information such as name or date of birth would require a new criminal and security check, as well as a new attestation of the accuracy of the data submitted. Therefore, the system cannot allow the customer to automatically update this important information once the adjudication process has started. USCIS does mitigate this risk by allowing the adjudicator to consider written requests to change this information, or an in-person appointment, at his or her discretion within established SOPs. The risk that a customer is unable



to correct an error he or she generated is mitigated by the USCIS data quality and integrity procedures within the adjudication process.

Privacy Risk: There is a risk that customers may be unable to access, correct, or amend their records because the systems used for criminal and national security background checks are exempt from the Privacy Act.

Mitigation: Due to the sensitive nature of criminal and national security background checks, customers are not provided with direct access to such records. For many lines of business, the customer has a formal appeals process through legacy processes for challenging decisions that they believe to be unfair or based on incorrect information.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ELIS has a sophisticated role-based user access for operational users as well as read-only users. These include roles that separate duties for operators to ensure appropriate oversight of the adjudication, as well as two levels of read-only roles to protect more sensitive data about a customer from being accessible to internal users who only have a need for some of their data. Additionally, USCIS ELIS captures all user activity, including information changed as well as viewed, in audit logs, which are reviewed by USCIS OSI.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

USCIS trains each USCIS ELIS user on proper handling of PII as well as appropriate use of data according to each role. Additionally, all USCIS employees receive privacy and security training annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

USCIS ELIS has several levels of operator roles as well as two levels of read-only roles. The operator roles are only available to individuals trained and currently occupying specific jobs within USCIS, and their supervisors are required to certify that their official duties align with the role before it is granted to those individuals. Likewise, USCIS will default to assigning the lower-



level of read-only to users requesting that access, unless they certify with supervisor confirmation that they need to know certain sensitive data about customers as part of their routine official duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS ELIS data would be subject to the USCIS formal review process for any data sharing agreements. That process includes, at a minimum, review by the Privacy Office, Counsel, and program officials entrusted with security of the data.

Responsible Officials

Donald Hawkins
Privacy Officer, U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Jonathan R. Cantor
Deputy Chief Privacy Officer
Department of Homeland Security



Appendix A

Immigration Benefit Types Processed in USCIS ELIS

Name of Immigration Benefit Type	Associated Forms and/or Collections	Paper Filings	Online Filings
Replacement of Permanent Resident Card	I-90	X	X
Deferred Action for Childhood Arrivals	I-821D, I-765, I-765WS	X	
USCIS Immigrant Fee	OMB Control Number 1615-0122 (not a form), DoS Immigrant Visa Packet (includes data from DS-260 and I-864)	N/A	X