Privacy Impact Assessment
for the

FOIA Immigration Records System (FIRST)

DHS/USCIS/PIA-077

March 20, 2019

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), operates the Freedom of Information Act (FOIA) Immigration Records System (FIRST) to process FOIA requests, Privacy Act requests, and Privacy Act amendment requests from any eligible person or entity requesting access to or amendment of USCIS records. FIRST serves two purposes: (1) FIRST has a public-facing portal that allows members of the public to submit FOIA/Privacy Act requests online and allows USCIS to electronically deliver responsive records, and (2) FIRST is an internal case management system for USCIS. USCIS is conducting this Privacy Impact Assessment (PIA) to analyze the privacy impacts associated with USCIS' use of FIRST, as well as the information collected, used, maintained, and disseminated.

Overview

U.S. Citizenship and Immigration Services (USCIS) administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting and securing the homeland. USCIS records take many forms, such as decision papers, Alien Files, memorandums, databases, audio and video recordings, publications, web pages, telephone logs, and email messages. Like all federal agencies, USCIS discloses information as permitted under the Freedom of Information Act (FOIA)[1] and Privacy Act of 1974[2] (hereinafter referred to as Privacy Act) upon receiving a written request.

FOIA and the Privacy Act have different purposes. FOIA permits any person to request access to federal agency records. FOIA establishes a presumption that records in the possession of federal departments and agencies are accessible, except to the extent that the records are protected from disclosure by any of the nine exemptions contained in the law or by one of three special law enforcement record exclusions. The Privacy Act can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. It was created to protect information about individuals from disclosure to third parties while allowing them the right to access information about themselves, request amendment or correction of those records, and request an accounting of disclosures of their records by the agency. FOIA requires federal agencies to disclose any information requested unless it falls under one of nine exemptions, which protect interests such as personal privacy, national security, and law enforcement. Individuals, as defined under the Privacy Act as U.S. citizens and lawful permanent residents, may request to access or amend Privacy Act-protected records about themselves. However, depending on the nature of the record, it may be exempt from access and amendment provisions of the Privacy Act.[3] When

[1] 5 U.S.C. § 552.
[2] 5 U.S.C. § 552a.
[3] 5 U.S.C. §§ 552a(j), (k).

individuals request records about themselves from the Federal Government, USCIS, like all agencies, applies both the FOIA and the Privacy Act to grant the most access possible.

Additionally, the Judicial Redress Act of 2015 (JRA) amended the Privacy Act to allow citizens of designated foreign countries or regional economic integration organizations to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests.[4] The Department of Homeland Security (DHS) and its components are a designated federal agency under the JRA; therefore, persons covered by the JRA can make access and amendment requests for covered records held by USCIS. The JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

All FOIA requests, Privacy Act access requests, and Privacy Act amendment requests for USCIS records are centralized at the National Records Center (NRC) within the FOIA Operations Division. The FOIA Operations Division processes all USCIS requests for records (including all Alien Files) and information requested under the disclosure provisions of the FOIA[5] and the Privacy Act (including the JRA).[6] USCIS manages its FOIA/Privacy Act program in accordance with the FOIA, the Privacy Act, DHS regulations, and DHS policy. The USCIS centralized FOIA Operations Division receives, tracks, and processes all USCIS FOIA and Privacy Act requests to ensure transparency within the agency.

FOIA/Privacy Act Information Processing System (FIPS)

The FOIA Operations Division uses an electronic case management system to create, control, and process all incoming FOIA/Privacy Act requests. The FOIA Operations Division has historically used the legacy FOIA/Privacy Act Information Processing System (FIPS) to manage the FOIA/Privacy Act lifecycle for USCIS. FIPS primarily supported the management of paper-based FOIA/Privacy Act requests. As part of an agency-wide modernization effort, USCIS is moving to receive and respond to FOIA/Privacy Act requests electronically. When evaluating options for new IT deployments, the Office of Management and Budget (OMB) requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. In support of this initiative, USCIS migrated records from the legacy FIPS to a cloud platform and renamed it to the FOIA Immigration Records System (FIRST).[7] FIRST operates on the Amazon Web Services (AWS) cloud platform. FIRST continues to support internal case

[4] More information regarding the Judicial Redress Act of 2015, 5 U.S.C. § 552a note, is available at https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.
[5] The Freedom of Information Act of 1966, as amended, permits any person to request access to federal agency records. FOIA establishes a presumption that records in the possession of federal departments and agencies are accessible, except to the extent that the records are protected from disclosure by any of the nine exemptions contained in the law or by one of three special law enforcement record exclusions.
[6] 5 U.S.C. § 552a(b). Records may be exempt from the access and amendment provisions of the Privacy Act. *See* 5 U.S.C. §§ 552a(j), (k).
[7] USCIS is undergoing a system modernization effort to align with the Cloud Smart initiative. Cloud Smart is a new strategy for agencies to adopt cloud solutions that streamline transformation and embrace modern capabilities.

management functions for the FOIA/Privacy Act lifecycle like the legacy FIPS. With the publication of this PIA, USCIS plans to retire the FIPS PIA and all associated updates.

FIRST is also part of USCIS' ongoing effort to move the nation's legacy immigration system away from paper-based services to digital transactions. FIRST includes a public-facing portal, which allows requesters to submit, manage, and receive FOIA/Privacy Act requests entirely online. Before this expansion, USCIS only accepted FOIA/Privacy Act requests by mail, fax, and email, and requesters typically received their documents on a compact disc by mail. FIRST offers a fully electronic service to requesters, which includes online request submission and online receipt of responsive records. FIRST aims to reduce the time and expense associated with receiving and responding to paper requests for both USCIS and requesters.

FOIA Immigration Records System (FIRST)

FIRST is a cloud-based technology to electronically support the FOIA/Privacy Act request process for requesters and the FOIA/Privacy Act management needs of USCIS. FIRST serves two main purposes:

1. To support the document imaging and workflow to manage the FOIA/Privacy Act case lifecycle for USCIS. USCIS permits requesters to access records, by: (1) completing Form G-639, *Freedom of Information Act/Privacy Act Request*; (2) sending a written letter by mail, fax, or email; or (3) submitting a request utilizing the electronic Form G-639 through the FIRST online portal. Requests submitted by mail, fax, or email are scanned into FIRST. USCIS reviews the documents and enters the information provided by the requester into the database. Then, the request is uploaded into FIRST by manually inputting the data fields provided by the requester and assigning a computer-generated case control number that is used for tracking purposes; and
2. To allow requesters to submit, manage, and receive FOIA/Privacy Act requests and responses entirely online. Requests submitted through the FIRST online portal are indexed by auto-populating the data fields provided by the requester and assigned a computer-generated case control number that is used for tracking purposes.

FIRST as a Public-Facing Portal

USCIS is launching the FIRST public-facing portal for FOIA requests, Privacy Act access requests, and Privacy Act amendment requests. Currently, requesters can use a completely electronic FOIA/Privacy Act system, from submitting requests online to retrieving and downloading documents to other case-related administrative actions, all of which eliminate the time and expense associated with receiving requests by mail. Through their account, requesters can track the status of their FOIA/Privacy Act requests and receive email notifications when USCIS has uploaded their responsive records. USCIS will update this PIA as additional services become available.

Account Creation

To submit a FOIA/Privacy Act request online or receive responsive records through the FIRST Digital Release portal for a mailed, faxed, or emailed request, the requester must have a USCIS online account. FIRST leverages Accounts Public, which is the enterprise-wide program that manages identity, credential, and access for USCIS online accounts. Accounts Public provides the general public with access to USCIS external-facing systems. Requesters with an existing USCIS online account are able to use their current account login and password information to log in to FIRST. However, if the requester's USCIS online account becomes inactive, then the requester would be required to reactivate his or her USCIS online account to gain access to FIRST. If the requester does not have a USCIS online account, he or she is required to create one in order to file the request online.

To create an account, the requester enters an email address into an online form. USCIS sends a confirmation email to the provided email address to verify the email address. Once verified, the email address is then stored as the requester's user name. The requester is then directed to create a strong password, and provide "fill-in-the-blank" answers to security questions in case he or she needs to reset the account password. USCIS provides the requester with a dropdown menu of standard questions, and the requester chooses which ones to answer as security questions. USCIS does not use the answers to these questions for purposes other than assisting with password resets.

USCIS online account passwords and answers to the security questions are centrally stored within Accounts Public. Passwords are not visible to USCIS. The answers to the security questions are only visible to USCIS customer help desk personnel who assist with password resets.

Multi-Factor Authentication

The USCIS online account is created through Accounts Public and connects to FIRST without sharing any account information. FIRST leverages Accounts Public's authentication services[8] in order to provide high confidence that the requester controls the authenticators bound to the USCIS online account, such as email address, mobile phone number, or third-party authenticator application (e.g., Google Authenticator, Authy, Microsoft Authenticator).

The account holder can use any third-party authenticator application available on the device of his or her choice. If the account holder chooses to use a third-party authenticator application, he or she is provided instructions on how to connect to the third-party authenticator application. The selection and use of a third-party authenticator application is at the discretion of the account holder. USCIS does not prescribe a specific authenticator application. A separate

[8] Authentication is the process or action of verifying the identity of an account holder. Credentials that the account holder provides are compared to those on file. If the credentials match, the account holder is granted authorization for access.

USCIS notice advises the account holder to review the privacy policy of the third-party authenticator application since USCIS has no control over the third-party policies. The user credentials are sent to Accounts Public for verification and authentication.

To complete account creation and access to FIRST via Accounts Public, USCIS requires proof of possession and control of two distinct authentication factors through secure authentication protocols. Each time the requester logs in, FIRST forwards an authentication code (i.e., a one-time PIN) through an email, text message, or through the use of a third-party authenticator application to be used as a second factor in authenticating. The user credentials are sent to the Accounts Public system for verification and authentication.

Online Request Submission Requirements

FIRST allows requesters to submit a request online for FOIA/Privacy Act records and make a record amendment request (while also tracking all requests that come to USCIS through mail, fax, or email). Requesters can also submit appeals in response to how USCIS initially handled its response to a FOIA/Privacy Act request. For online request submissions, the requester is required to complete the Form G-639,[9] which is electronically replicated in FIRST.[10] Through the Form G-639, the requester may make a request for his or her own records (self), a request on behalf of someone else,[11] a request for someone else's records (third-party requests), an amendment request, or other information requests (e.g., procedural manuals, employment selections, training manuals, and contracts).

The Form G-639 is divided into five parts with each part collecting pertinent information, when required, to fulfill the FOIA/Privacy Act request or amendment request. These parts include:

1. **Type of Request** describes whether the request is an access request or an amendment request.
2. **Requester Information** collects name, mailing address, telephone number, email address, and signature.
3. **Description of Records Requested** collects information about the request and the subject of record. Requesters are required to reasonably describe the information being requested. This is facilitated by a drop down menu of options for the requester to select from, such as "naturalization certificate," "deportation records," "entire file," or "other" in which the requester can type in a description of the documents he or she is

[9] *See* https://www.uscis.gov/g-639.
[10] The Form G-639 is an optional form outside of FIRST (i.e., when submitting a FOIA/Privacy Act request through mail, fax, or email), but the requester is required to complete it in order to submit a FOIA/Privacy Act request through FIRST.
[11] Examples of a requester making a request on behalf of someone else include an attorney, accredited representative, documented guardianship, parents with birth certificate for minors, and power of attorney.

requesting. Information collected about the subject of record may include name, other names used (including nickname, alias, and maiden name), Form I-94 number, Alien Number (A-Number), USCIS Online Account Number, Receipt number, and parents' names or names of other family members.

4. **Verification of Identity and Subject of Record's Consent** collects information to verify the identity of the subject of record and the subject of record's consent (if applicable), including the subject of record's name, current address, date of birth, country of birth, and signature (as outlined in 6 CFR § 5.21(d)). It is optional to include the subject of record's telephone number and email address.
5. **Additional Information** allows the requester to provide additional information to help the FOIA Operations Division identify and locate records more expeditiously.

Requests for records that are not subject to the Privacy Act do not generally involve collecting a signature or consent as any potential responsive records generally will not contain PII. The requester's name, address, telephone number, or email address is the only information collected for these types of requests.

The amount of information collected and requirements for the Form G-639 is dependent on the type of request. Not every data field listed above in the Form G-639 is required to meet the identity verification requirements outlined in 6 CFR § 5.21(d); however, requesters may also submit additional information to help USCIS facilitate the processing of the FOIA/Privacy Act request in the most efficient manner. For records pertaining to an individual, in order for USCIS to verify the information submitted by the requester against the information contained within USCIS records, the requester must provide the subject of record's full name, current address, date of birth, and place of birth. This information is matched to information in the immigration file to verify the subject of record's identity, and the verification is documented in a case note within FIRST.

Before submitting the FOIA/Privacy Act request, the requester is given the opportunity to review and/or edit his or her request. Once the FOIA/Privacy Act request is officially submitted to USCIS, FIRST routes the request to be placed in an internal assignment queue on the case management aspect of FIRST.

Conditions for Release of Information

Prior to submitting the Form G-639 to USCIS, if the requester is the subject of record, he or she must electronically sign the request and the signature must be either notarized or submitted under 28 U.S.C. § 1746, in which the requester represents that the information provided is true and correct under a law that permits statements to be made under penalty of perjury as a substitute for notarization. Alternatively, the requester can upload a signed penalty of perjury statement or a notarized signature.

In order for USCIS to provide the greatest disclosure possible for a requester making a request on behalf of someone else or for a third-party requester seeking an individual's immigration records, the requester should provide consent and verification of identity information from the subject of record or proof of death. Such information will not be disclosed without that individual's prior written consent and verification of identity, unless the information is required to be released under the FOIA.

In certain cases in which a requester represents that he or she is seeking records on behalf of the subject of record and elects to have the subject of record provide consent directly through FIRST, USCIS contacts the subject of record to obtain consent. The subject of record receives a link to the request through FIRST and enters his or her date of birth and country of birth in order to view the request. The subject of record may review, change, and provide consent either electronically or through an uploaded document.

Digital Release Portal

USCIS also provides requesters who submit requests via mail, fax, or email with the option of receiving the responsive records through the Digital Release portal within FIRST, as opposed to receiving them by CD or in paper form. If the requester does not opt-in to receiving responsive records online, the records are mailed to the requester on a CD. To receive the responsive documents online, the requester must opt-in to the electronic process by linking the FOIA/Privacy Act request to his or her USCIS online account; otherwise, the process defaults to receiving responsive documents through the current mail process.

The Digital Release portal serves as an electronic repository for responsive records and correspondence created by USCIS. Responsive records are all records that fit within the scope of the requester's FOIA/Privacy Act request. USCIS responds to electronically submitted FOIA/Privacy Act requests by uploading the responsive records into the Digital Release portal. Requesters receive an email notification when the responsive records are available in the Digital Release portal. Responsive records are pushed through a one-way encrypted secured socket layer to the Digital Release portal. Information within the requester's FIRST portal can only be accessed by the requester within his or her account. This digital delivery process improves operational efficiency, and eliminates potential errors that can occur with manually issuing a CD.

Responsive records available in the Digital Release portal are automatically archived after 90 days. Requesters also have the ability to self-archive responsive records, which removes the records from the requester's active list. The requester can also unarchive responsive records to his or her active list. For responsive records that have been available for viewing in the Digital Release portal for more than six months beyond the original availability date, the requester is provided a message, prior to viewing the responsive records. The message states that the responsive records he or she is about to view are only current as of the date the request was made. The requester is

then asked, given the age of the records, if he or she wants to proceed.

FIRST as an Internal Case Management System

The USCIS FOIA Operations Division has a responsibility to track and monitor all incoming FOIA/Privacy Act requests to ensure USCIS complies with the statutory requirements associated with responding to requests. USCIS is also required to conduct a search for responsive records and release those records unless an exemption applies. The FOIA Operations Division uses FIRST as an internal case management system to manage all FOIA/Privacy Act requests for USCIS. USCIS employees can also use FIRST to search for any duplicate cases[12] and can move a case to various work queues until the case is ready to be closed or initiate a search for responsive records. Employees are able to review and process electronic documents responsive to FOIA/Privacy Act requests to determine and apply appropriate FOIA or Privacy Act exemptions.

Case Creation

USCIS processes FOIA, Privacy Act, and Privacy Act amendment requests on a first-in, first-out basis. Once USCIS receives the request, the request is placed in the case creation queue within FIRST. The information provided by the requester is entered into FIRST and used to create a case. Each case is assigned a system-generated case control number. The case control number is generated based on sequential order as the cases are created. The queue is in sequential order of submission of the request. The employee is automatically assigned the next request in line.

All FOIA/Privacy Act requests are routed to the FOIA Operations Division or the Significant Interest Group (SIG) for processing. The FOIA Operations Division is responsible for processing self-requests, requests on behalf of someone else, and third-party requests for requesters seeking Alien File documents. SIG is responsible for processing all other information requests, such as requests for personnel records, contracts, and statistics. Once appropriately routed, each case is reviewed to ensure all applicable sections of the request are properly completed to be processed. For self-requests, requests on behalf of someone else, and third-party requests, the employee verifies that all required information is present as outlined above in the *Online Request Submission Requirements* section. USCIS uses the information to identify and locate the specifically requested material. This information is also matched to information in the actual file to verify the requester's identity. If the request is not completed correctly (e.g., a date of birth is missing or incorrect), then the employee closes the case using the correct code and generates a final action letter explaining why the request was closed. The case is then routed to a lead or supervisor in the approval queue for verification that the case was appropriately handled.

[12] The employee searches for duplicate cases by entering the subject of record's name to see if there has been another request for the same information by the same requester.

Acknowledgment Letter

After a request is submitted, the USCIS employee generates an acknowledgment letter in FIRST. The letter informs the requester that his or her request has been received and provides the requester with the case control number that is used on all further correspondence concerning the request. Depending on the method the requester used to file the request, USCIS either uploads the letter in the Digital Release portal or responds by mail. When a FOIA/Privacy Act request is submitted online through FIRST, the employee uploads the acknowledgment letter into the Digital Release portal in FIRST. The requester gets an email notification when the acknowledgment letter is available in the portal.

When a FOIA/Privacy Act request is submitted by mail, fax, or email, a case number is assigned to the request, and the employee generates an acknowledgment letter that is sent to the requester via the United States Postal Service (USPS) to the postal address listed on the request. The acknowledgment letter lists two options available for the requester to receive responsive records (i.e., through the Digital Release portal or through USPS mail). If the requester prefers to receive responsive records online, the requester must opt-in for an online delivery by actively registering his or her FOIA/Privacy Act request to his or her USCIS online account. The acknowledgment letter provides instructions for (1) creating a USCIS online account for viewing and retrieving the responsive records, and (2) using the control number and a Personal Identification Number (PIN) to associate the USCIS online account to responsive records within FIRST.[13]

Records Search Process

In addressing FOIA/Privacy Act requests for an individual's Alien File[14] (also known as the A-File) or other immigration records, USCIS employees search for records responsive to the request by using other USCIS systems that house official immigration records. FIRST has a direct connection with RAILS,[15] Enterprise Document Management System (EDMS),[16] Content Management Services (CMS),[17] and USCIS Electronic Information System (USCIS ELIS).[18]

[13] Currently, the PIN does not expire if the requester does not opt-in to electronic delivery. However, if the requester does not opt-in, the responsive records are sent via mail, and there would be no records in the Digital Release portal for the requester to view if he or she accessed the portal at a later date.
[14] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017). The purpose of the A-File is to document and maintain the official record of an individual's immigration applications, petitions, and requests, as well as enforcement transactions as he or she passes through the U.S. immigration process. The official records in the A-File consist of paper and electronic records of the individual's transactions through the immigration process, including records of immigration benefit requests and requests for agency action filed with USCIS, but does not include all case processing and decisional data.
[15] RAILS is not an acronym. *See* DHS/USCIS/PIA-075 RAILS, *available at* https://www.dhs.gov/privacy.
[16] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/privacy.
[17] *See* the forthcoming CMS PIA for more information, *available at* https://www.dhs.gov/privacy.
[18] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* https://www.dhs.gov/privacy.

FIRST searches for the A-File using the A-Number to retrieve records within RAILS. In turn, RAILS displays the types of files available and at which File Control Office (FCO) they are located. If records are located, the employee selects the appropriate file(s) to request, and a pull ticket is generated and placed in the FCO transfer queue for the file to be sent to the FOIA Operations Division. Records maintained in EDMS and USCIS ELIS are directly transferred to FIRST through an application program interface connection. If no responsive records are located or do not fall under the jurisdiction of USCIS, the employee closes the case using the appropriate code and generates a final action letter. The case is routed for approval.

All responsive records are stored in CMS, which operates as the backend repository for the management of FOIA/Privacy Act requests. FIRST integrates with CMS to retrieve immigration related content used to respond to FOIA and Privacy Act requests, as well as to store the redacted and non-redacted FOIA/Privacy Act responsive records. FIRST retrieves the responsive records from CMS in order for employees to view the records within FIRST. Documents in CMS are encrypted during storage and when being displayed within FIRST.

Manual Records Identity Verification

As part of the FOIA/Privacy Act review process, USCIS verifies the information submitted by the requester against the information contained within USCIS records. The employee verifies that the required information from the case creation is included and matches information from the requested file with the subject of record's information from the request to ensure the correct records are attached. Individuals submitting FOIA/Privacy Act requests may submit all or some of the following information:

- Name;
- Date of Birth;
- Current Address;
- Phone Numbers (e.g., phone, fax, and cell);
- Vital Certificates (e.g., birth, death, and marriage);
- Email Address;
- A-Number; and
- Country or Place of Birth.

This information, which is provided directly by the requester, is either auto-populated or manually entered into FIRST and then manually verified by locating the information in the A-File that was submitted on the Form G-639. The only mandatory information for identity verification purposes is the subject of record's name, current address, date of birth, and place of birth. Any additional

information provided, such as phone number, fax number, vital certificate (e.g., birth, death, and/or marriage), email address, or A-Number, is used to help the FOIA Operations Division identify and locate records more expeditiously. Please note that USCIS does not request Social Security numbers (SSN), and requesters are not required to submit such information.

Responsive Record Review Process

Once the responsive records are ingested into FIRST, the case is automatically routed to the appropriate processing track for the employee to process. These tracks include:

1. Track 1 – specific document requests
2. Track 2 – entire A-File requests
3. Track 3 – requests from requesters with scheduled immigration court dates

Employees are assigned to the specific tracks within FIRST and can only work on a case that is in the specific track assigned to them. These tracks are assigned and managed by the supervisor.

Once a case is ready for processing, the employee is assigned the next available case from the track queue that he or she is assigned to work. For all tracks, the employee begins processing a case by verifying that the required information from the case creation is included and matches information from the requested file with the subject of record's information from the request to ensure the correct records are attached.

Processing the records is also consistent across the tracks. The employee reviews each page of the responsive records and applies any applicable redactions pursuant to the FOIA and the Privacy Act (when applicable). Pages may also be referred to other agencies or components for processing if the information does not belong to USCIS. Employees can also submit a case to an administrative queue for questions or assistance by their supervisor. All redactions and referrals are automatically tracked and saved in FIRST for reporting purposes.

Approval Process and Responding to FOIA/Privacy Act Requests

Once all pages have been processed, the employee creates a final action letter using the appropriate code. FIRST generates automated response letters including blank,[19] expedited processing denial, final action, still interested,[20] payment, redirect, referral, referral memo to a DHS component, remand memo, specialty (lost file and Track 3 denials),[21] status, and

[19] Blank letters allow for FOIA/Privacy Act staff to customize letters based on specific situations.
[20] USCIS uses "still interested" letters in limited situations in which USCIS has a reasonable basis to conclude that the requester's interest in the records may have changed.
[21] Track 3 is for cases with scheduled immigration court proceedings. Track 3 denial letters are considered specialty letters that inform the requester that his or her request has been denied.

supplemental release letters.[22]

Once the employee completes the final action letter, the case is sent to the approver's queue. The approvers have cases assigned to their work queues based on their specific track responsibilities. The approvers review the case and, if correct, the case is closed and the responsive records and final action letter are sent for printing or uploaded into the Digital Release portal. Pages referred to other agencies or components are printed and sent via mail. If the case is not correct, the case is returned to the employee for correction or fixed by the approver.

After the final review of the responsive records is complete, the employee sends the final action letter with the responsive, non-exempt records to the requester in one of the following ways:

1. Through the mail, FIRST can either save the responsive records to a CD and provide that CD to the requester or return the responsive records in paper format.
2. FIRST can also deliver responsive records through the Digital Release portal for requests sent by mail, fax, or email. All responsive records for requests submitted online through FIRST are automatically delivered via the Digital Release portal.

Appeals and Litigation Processing

If a requester receives his or her responsive records and wishes to challenge USCIS' handling of or response to a FOIA/Privacy Act request (e.g., the use of FOIA exemptions or finding no responsive records), he or she can file an appeal within 90 days from the date of the final action letter. Requesters can submit appeals online through the FIRST portal or through fax, email, or mail. Once an appeal is received, it is forwarded to the appeals unit and a case is created in the appeals queue within FIRST. FIRST generates an appeals case number, and the employee creates and sends an acknowledgement letter to the requester. The redacted and unredacted responsive records from the original release are retrieved from CMS and uploaded to the case.

The appeals employee reviews the case and makes any necessary changes. Once completed, the appeals employee generates a final action letter and sends the case to the approver. Upon review and approval, the case is closed, and the final action letter and related documents, if applicable, are uploaded to the Digital Release portal or printed to a CD and mailed. Similar to the process as described above, all redactions and changes to the case are tracked in FIRST for reporting purposes.

Cases in litigation are flagged and are only accessible to USCIS FOIA personnel and USCIS Office of Chief Counsel personnel involved in the litigation. Cases in litigation are still processed on a first-in, first-out basis; however, these cases are flagged within FIRST to preserve the records for litigation purposes. Once the litigation is completed, the records are maintained per

[22] A supplemental release is when USCIS responds after an initial response was sent out. More documents may have been discovered and processed or documents may have been reprocessed.

the National Archive and Records Administration (NARA) General Records Schedule 4.2.

Automated Reports

FIRST generates automated reports. The automated reports are categorized according to the type of information they present. The following reports are for internal management use only:

- Appeals reports to manage and report on appealed cases (contains PII);[23]
- Balanced Scorecard reports to report balanced scorecard metrics to help with strategic goals for customer service and resources;
- Detailed reports provide case lists of pending, unassigned cases (contains PII);[24]
- Management reports to help managers monitor workloads, determine resource needs, and recognize problem areas;
- Summary reports to provide management and analysis information;
- Troubleshooting reports to identify potential problems; and
- Employee dashboards, which display "real time" personal statistics.

FIRST also helps the FOIA Operations Division prepare the data needed for annual reports for DHS annual reporting requirements, such as the FOIA Annual Report.

Audits

FIRST tracks all access, modifications, and updates to the data. Each case maintains a log of all actions taken for the case, including dates, times, and IDs of the person accessing the record. These logs are kept in each individual case and remain with the case until the case is deleted per the NARA schedule. Additionally, there are logs for the type of reports that are generated, including the same information listed above. These logs can be used to provide an audit, if needed to ensure that correct information is being maintained, as well as to verify correct user roles and access.

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 Freedom of Information Act of 1966, as amended (5 U.S.C. § 552), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), 5 U.S.C. § 301, 6 CFR Part 5, and 44 U.S.C. § 3101 authorize

[23] This report contains the name of the appellant, the name and A-Number of the individual whose case is part of the responsive record, and the name of the FOIA Operations Division employee who processed the request.
[24] This report contains the name of the requester, the name and A-Number of the individual whose case is part of the responsive record, and the name of the FOIA Operations Division employee who processed the request.

the collection of this information.

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

The information collected, used, maintained, and stored in FIRST is covered under DHS/ALL-001 DHS FOIA and Privacy Act Record System[25] and DHS/ALL-037 E-Authentication Records System of Records.[26] The DHS/ALL-001 DHS FOIA and Privacy Act Record System SORN covers the collection, maintenance, and use of the information to support the processing of record access requests and administrative appeals under the FOIA, as well as access, notification, and amendment requests and administrative appeals under the Privacy Act. The DHS/ALL-037 E-Authentication Records System of Records SORN covers information collected to create and authenticate an individual's identity for the purpose of obtaining a credential to electronically access FIRST.

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

As stated earlier, FIRST is a modernization of FIPS. Since FIPS was a part of the Ongoing Authorization program, it had a continuous authority to operate (ATO). Therefore, a new ATO is not needed for FIRST. However, each phase of modernization must be fully documented and assessed to ensure the security posture of the system. Ongoing Authorization requires FIRST to be reviewed on a monthly basis to ensure compliance with security and privacy requirements in order to maintain its ATO.

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

Yes. Records in FIRST are subject to NARA General Records Schedule 4.2: Information Access and Protection Records (January 2017), which mandates that records are maintained for a period of 6 years from the final agency action or 3 years after final adjudication by the courts, whichever is later.

[25] *See* DHS/ALL-001 DHS FOIA and Privacy Act Record System, 79 FR 6609 (February 4, 2014).
[26] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

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 requesting access to information under the FOIA and Privacy Act is 1615-0102, which corresponds to USCIS Form G-639, *Freedom of Information Act/Privacy Act Request*.[27]

Section 2.0 Characterization of the Information

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

FIRST stores three categories of information: (1) biographical data given to USCIS from the requester, such as the requester's or the subject of record's name, address, and A-Number; (2) correspondence to and from the requester and with federal offices; and (3) electronic images of USCIS records that are responsive to the FOIA/Privacy Act request. FIRST also includes indexing information, such as case and document control numbers (within the system) and classification information, such as the source and type of the request. None of the information is shared with other systems.

Biographical Data

The PII that requesters submit with their FOIA/Privacy Act requests to USCIS depends on the substance of the request. USCIS may collect the following searchable information:

- Requester and Subject of Record Name(s);
- Requester Business and/or Personal Address(es), as applicable;
- Requester Business and/or Personal Phone Number(s), as applicable; and
- Requester and Subject of Record A-Number, as applicable.

When individuals seek records from a USCIS system of records or any other DHS system of records, their request must conform to the FOIA/Privacy Act regulations set forth in 6 CFR part 5. In the case of first-party requesters and requesters seeking immigration records on behalf of an individual, in order for USCIS to verify the information submitted by the requester against the information contained within USCIS records, USCIS generally collects the subject of record's full name, current address, date of birth, place of birth, and signature. Requesters are also required to reasonably describe the information being requested. Individuals may also submit additional

[27] The Form G-639 and submission instructions are available at https://www.uscis.gov/g-639.

information, such as phone number, fax number, vital certificate (e.g., birth, death, or marriage), email address, or A-Number, to help the FOIA Operations Division to identify and locate records more expeditiously. USCIS does not request SSNs, and individuals are not required to submit such information.

Information in Responsive Records

FIRST also maintains records responsive to FOIA/Privacy Act requests in a non-searchable format. The information contained in responsive FOIA/Privacy Act documents can vary depending on what information is requested. The information may include the following: names, addresses, phone numbers, fax numbers, zip codes, email addresses, A-Numbers, SSNs (or other number originated by a government that specifically identifies an individual), other identifying numbers, fingerprints, date of birth, country of birth, mother's maiden name, driver's license, birth records, marriage records, passport records, death records, tax records, educational records, financial records, civil or criminal history information, biometric identifiers (e.g., fingerprints), vehicle identifiers (e.g., license plates), photographic identifiers (e.g., photograph images and video tapes), and/or other records maintained by USCIS. In addition, FIRST maintains records responsive to other non-A-File information requests related to statistics, contracts, memoranda, etc.

Audit Data

FIRST will also collect the employee and contractor user IDs for audit purposes to ensure that correct information is being maintained, as well as to verify correct user roles and access.

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

The sources of information for FOIA/Privacy Act requests include the following:

- Individuals who submit FOIA/Privacy Act requests;
- Individuals who subsequently appeal USCIS' denial of their FOIA/Privacy Act requests;
- Individuals whose requests, appeals, and records were referred to USCIS by other agencies; and
- Attorneys or other persons representing the individual submitting such requests and appeals.

The sources of the information for responsive records can be from a variety of systems, including the A-File, EDMS,[28] USCIS ELIS,[29] Computer Linked Application Information

[28] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/privacy.
[29] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* https://www.dhs.gov/privacy.

Management System (CLAIMS 3),[30] Central Index System (CIS 2),[31] RAILS (formerly the National File Tracking System),[32] and CMS.[33]

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.

Information received by USCIS from individuals submitting FOIA/Privacy Act requests is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. There are three levels of review that take place to ensure accuracy of information entered into FIRST, depending on what material is being requested. For A-File materials, the employee compares the information contained in the original request letter against the information contained in CIS 2. Then, the employee reviews and confirms that the PII contained in the responsive record matches the identifying information provided by the requester. This level of review is to assure that the correct requested record has been scanned into FIRST. Regardless of what type of record is requested, before a response is sent to the requester, all of the information and records are reviewed for accuracy by an approver (such as a supervisor). Should any inaccuracies be discovered during the resolution of the case file, USCIS may contact the originating submitter for clarification.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that non-essential information may be collected.

Mitigation: To mitigate this risk, USCIS only requires certain information when an individual submits a request, such as name, date of birth, place of birth, current address, and the FOIA/Privacy Act request itself (as consistent with 6 CFR part 5). FIRST has a help section that details what information the requester should submit. The requester can reference this help section if he or she needs any assistance when submitting a FOIA/Privacy Act request online. However, it is still possible the requester may submit more information than 6 CFR part 5 requires, which is outside the control of USCIS. All information submitted by the requester is protected and generally accessible only to FOIA Operations Division employees.

[30] *See* DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* https://www.dhs.gov/privacy.
[31] *See* DHS/USCIS/PIA-009(b) Central Index System, *available at* https://www.dhs.gov/privacy.
[32] *See* DHS/USCIS/PIA-075 RAILS, *available at* https://www.dhs.gov/privacy.
[33] *See* the forthcoming CMS PIA for more information, *available at* https://www.dhs.gov/privacy.

Privacy Risk: There is a risk that information collected from the requester or information contained within the responsive records may be inaccurate.

Mitigation: The risk of inaccuracy is reduced by collecting contact information directly from the individual requester or representative. Although the FOIA Operations Division depends on the originating office and relevant IT systems for the accurate responsive records, information entered into FIRST undergoes three levels of review to ensure the accuracy of information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FIRST serves two purposes: (1) FIRST is an internal case management system, and (2) FIRST has a public-facing portal that allows for the submission of online FOIA/Privacy Act requests and electronic delivery of responsive records.

USCIS uses FIRST as an internal case management system to administer USCIS' FOIA/Privacy Act program by tracking the FOIA/Privacy Act requests received. All information pertaining to the FOIA/Privacy Act request is contained within FIRST. Information received by USCIS from individuals submitting FOIA/Privacy Act requests is used to analyze, process, and respond to the request. Once received, the FOIA Operations Division records the request and then distributes it to the appropriate program office to conduct a search for the requested records. When an individual submits a request for records pertaining to an individual, PII provided by the requester may be used to assist the program office in conducting a search for responsive records. If records responsive to the request exist, they are analyzed for releasability and are enclosed with a letter to the requester itemizing the records and identifying what, if any, exemptions are claimed to withhold portions of the records either from the FOIA or the Privacy Act. If there are no responsive records, USCIS sends a letter to the requester advising him or her accordingly. FIRST generates reports to provide insight to NRC management that enables them to track the number and types of FOIA requests.

FIRST also has a public-facing portal that allows for the submission of online FOIA/Privacy Act requests and electronic delivery of responsive records. In order to establish an online account to receive responsive records, USCIS collects information related to the account, such as user name that is an email address (used to contact the individual), password, and challenge questions.

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?

There are also designated individuals within DHS components who have limited administrative rights in certain instances to log into FIRST to upload responsive materials directly into FIRST. These rights only apply for cases processed by the Significant Interest Group. The FIRST administrator will grant or deny access, in addition to auditing access requests.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that internal access to information may be unauthorized.

Mitigation: This risk is partially mitigated. The information contained in FIRST is used for the purpose of responding to FOIA/Privacy Act requests. Access to FIRST is only given to users who need it to perform their work. In addition, all users must be authenticated by user ID and passwords. Generally, only certain employees within the FOIA Operations Division, their contractors, and attorneys working on FOIA matters have access to information contained in FIRST. The FIRST administrator will grant or deny access, in addition to auditing access requests, thus ensuring that only those users with approved and assigned roles can search and process data and document images associated with any particular request.

Privacy Risk: There is a risk that an individual (that is not the requester) will gain unauthorized access to the requester's portal.

Mitigation: This risk is partially mitigated. There is a chance that an individual could intercept the acknowledgment letter that contains the control number and PIN. If the requester already has a USCIS online account, then the unauthorized individual would also have to know the requester's user name and password to gain access to the requester's portal in FIRST. If the requester does not have a USCIS online account, then that unauthorized individual could set up an account either to gain access to the requester's responsive records through the Digital Release portal or to submit a request posing as the requester. To mitigate this risk, USCIS uses multi-factor authentication. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols.

Privacy Risk: There is a risk that information may not be used for its intended purpose.

Mitigation: Employees within the FOIA Operations Division and their contractors are required to complete Computer Security Awareness Training, Privacy Act Training, and Records Management Awareness Training annually. All of the training programs address the responsibility of using USCIS data and records for their intended purposes only. In addition, DHS components are ultimately responsible for ensuring that data is used appropriately. This is done by the establishment of standard operating procedures that stipulate prescribed and permitted activities, uses, auditing requirements, and integrity controls.

Privacy Risk: There is a risk that FIRST will inadvertently disclose information about a different individual by uploading the incorrect FOIA/Privacy Act responsive documents to the Digital Release portal.

Mitigation: This risk is mitigated. The control number and PIN (as provided in the acknowledgment letter) used to link the responsive records to the requester are directly associated with the control number of the FOIA/Privacy Act request. Responsive records cannot be transferred to any other requester within the Digital Release portal.

Privacy Risk: There is a risk that USCIS will disclose information concerning a subject of record to a third-party requester when the individual's information is not required to be released.

Mitigation: This risk is mitigated. In order for USCIS to provide the greatest disclosure possible for a requester making a request on behalf of someone else or for a third-party requester, the requester should provide consent and verification of identity information from the subject of record or proof of death. In the absence of such consent or proof of death, USCIS will only disclose information concerning the subject of record if the information is required to be released.

Privacy Risk: There is a risk that there is no remote identity proofing process in place.[34]

Mitigation: This risk is not mitigated. The remote identity proofing process is currently being developed as part of USCIS' initiative to move from paper-based processes to digital transactions. USCIS will detail this process in a PIA Update. USCIS is not changing its current process for identity verification of the subject of record in regards to verifying the information submitted by the requester against the information contained within USCIS records. Individuals submitting FOIA or Privacy Act requests may submit all or some of the following information:

[34] Remote identity proofing is the online process of assuring that the individual is who he or she purports to be.

- Name;
- Date of Birth;
- Mailing Address;
- Phone Numbers (e.g., phone, fax, and cell);
- Certificates (e.g., birth, death, and marriage);
- Email Address;
- A-Number; and
- Country or Place of Birth.

This information, which is provided directly by the individual, is entered into FIRST and manually verified. USCIS will not release any information pertaining to an individual to the requester unless the information supplied by the requester matches the information in the subject of record's immigration file to verify the identity.

Section 4.0 Notice

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 general notice to individuals through this PIA, the DHS/ALL-001 DHS FOIA and Privacy Act Record System SORN,[35] and the DHS/ALL-037 E-Authentication Records System of Records.[36]

USCIS continues to provide notice to individuals through the associated Privacy Notices contained on Form G-639, *Freedom of Information Act/Privacy Act Request*, and the ICAM Public account creation webpage.[37] Each Privacy Notice provides notice to individuals about USCIS' authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS.

Furthermore, USCIS is providing notice through the acknowledgment letter sent to requesters upon receiving a FOIA/Privacy Act request and on USCIS' FOIA/Privacy Act webpage.[38] USCIS' FOIA/Privacy Act webpage details the information that USCIS needs to verify the information submitted by the requester against the information contained within USCIS records.

Lastly, USCIS has developed a public marketing strategy for FIRST, which includes press releases, social media outreach, and information included in the acknowledgement letters.

[35] *See* DHS/ALL-001 DHS FOIA and Privacy Act Record System, 79 FR 6609 (February 4, 2014).
[36] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[37] *See* https://myaccount.uscis.dhs.gov/.
[38] *See* https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/uscis-freedom-information-act-and-privacy-act.

Additionally, there will be a public engagement meeting/webinar with the public and stakeholders.

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

Individuals making a FOIA/Privacy Act request have an opportunity and right to decline to provide information. Submission of a FOIA/Privacy Act request is strictly voluntary. If an individual chooses to make a FOIA/Privacy Act request, then certain information about the subject of record is required to process the request in order for USCIS to verify the information submitted by the requester against the information contained within USCIS records. Failure to submit such information may delay USCIS' ability to provide responsive records or result in USCIS' inability to locate requested documents.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not have notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. USCIS is providing notice through the publication of this PIA. USCIS provides notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice that the information may be stored in a cloud-based system at the time of collection. Regardless of storage location of records, the records in FIRST are governed by the USCIS' information collection, use, and dissemination policies and procedures.

Section 5.0 Data Retention by the project

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

Records in FIRST are subject to NARA General Records Schedule 4.2: Information Access and Protection Records, which mandates that records are maintained for a period of 6 years from the final agency action or 3 years after final adjudication by the courts, whichever is later.

Responsive records available on the Digital Release portal will be automatically archived after 90 days. Requesters also have the ability to self-archive responsive records, which removes the records from the requester's active list. Responsive records may be restored to the active list by the requester. For responsive records that have been available for viewing in the Digital Release portal for more than six months beyond the original availability date, the requester is provided a message, prior to viewing the responsive records, that highlights the fact that the responsive records he or she is about to view are only current as of the date the request was made. The requester is then asked, given the age of the records, if he or she wants to proceed.

If the requester's USCIS online account becomes inactive, then the requester would be required to reactivate his or her USCIS online account to gain access to FIRST.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data may be retained longer than necessary.

Mitigation: This risk is mitigated. NARA General Records Schedule 4.2 is consistent with the concept of retaining data only for as long as necessary to support the operational integrity of USCIS' FOIA and Privacy Act program. To ensure data is properly disposed of or deleted at the end of the retention period, FIRST will automatically calculate and set the deletion date based on the date the request is closed.

Section 6.0 Information Sharing

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.

A portion or all of the information maintained in FIRST may be shared pursuant to the approved routine uses, including but not limited to the following:

- The Department of Justice (DOJ), including United States Attorney Offices, or other federal agencies conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation;
- A congressional office in response to an inquiry made at the request of the individual to whom the record pertains;
- A federal agency or other federal entity that furnished the record or information for the purpose of permitting that agency or entity to make a decision regarding access to or correction of the record or information, or for purposes of providing guidance or advice regarding the handling of particular requests;
- An agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function; and
- Federal, state, tribal, local, international, or foreign agencies, including law enforcement or other appropriate authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

In addition to those disclosures generally permitted under 5 U.S.C. § 552a (b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS in accordance with the routine uses found in DHS/ALL-001 DHS FOIA and Privacy Act Record System.[39]

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

The external sharing is compatible with the original collection. USCIS shares information with external organizations when required by statute, Executive Order, regulation, or policy and for the response of a FOIA/Privacy Act request. This coordination may be necessary to ensure that records requested, which are not DHS records, may be referred to and/or DHS may receive consultation from the applicable federal agency in order to respond. External organizations do not have access to the case management portion of FIRST.

Specifically, Routine Uses A, B, G, I, and L of the DHS FOIA and Privacy Act Record System SORN allow USCIS to share information with external organizations when required by statute, Executive Order, regulation, or policy and for the response of a FOIA/Privacy Act request.[40] Information may be shared with law enforcement, such as threatening correspondence directed at the Department or its employees, or if an opinion is sought from an attorney at DOJ on a particular matter of FOIA or Privacy Act law.

6.3 Does the project place limitations on re-dissemination?

No. If information is shared as a result of a routine use, there are no limitations on re-dissemination. In addition, once the responsive FOIA/Privacy Act records are released to the requester, USCIS cannot control re-dissemination. Also, in accordance with 6 CFR § 5.4, if USCIS erroneously receives a FOIA/Privacy Act request that was misdirected within DHS, the FOIA Operations Division routes the request to the appropriate DHS component. It is up to that component to address that FOIA/Privacy Act request. Furthermore, if USCIS either receives a request for non-DHS records or finds non-USCIS records that are responsive to a USCIS FOIA/Privacy Act request, the FOIA Operations Division may refer the request or records to another DHS component or the appropriate federal agency as long as that agency is subject to the FOIA. Once the request or records are referred, it is up the component or federal agency to address the processing and dissemination of the referred request or records.

---

[39] *See* DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, 79 FR 6609 (February 4, 2014).
[40] *See* DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, 79 FR 6609 (February 4, 2014).

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

FIRST tracks all access, modifications, and updates to the data. Each case within FIRST has comprehensive audit logs that maintain all actions taken for the case, including disclosures outside the Department in the case when pages that are referred to other agencies, to prevent the misuse of data. The audit logs capture user, date, time, and data accessed. These logs are used to generate reports to account for all disclosures of information through the FOIA/Privacy Act process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information may be shared with agencies or other entities that do not have a need to know.

Mitigation: This risk is mitigated. FIRST managers have the ability to review audit logs for inappropriate external information sharing in accordance with USCIS procedures. USCIS only shares information with external organizations when required by statue, Executive Order, regulation, or policy or for the response of a FOIA/Privacy Act request. Information may also be shared with law enforcement, such as threatening correspondence directed at DHS or its employees, or if an opinion is sought from an attorney at DOJ on a particular matter of FOIA or Privacy Act law. These instances of sharing are fully consistent with the DHS/USCIS-001 DHS FOIA and Privacy Act Record System SORN.[41]

Section 7.0 Redress

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

FIRST supports an individual's ability to access to his or her USCIS records by filing a Privacy Act or FOIA request and viewing those records online. Only U.S. citizens, lawful permanent residents, and individuals covered by the JRA may file a Privacy Act request. Individuals not covered by the Privacy Act or the JRA still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Any person, regardless of immigration status, may file a FOIA request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS records, he or she may mail the request to the following address:

[41] *See* DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, 79 FR 6609 (February 4, 2014).

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

Some information requested may be exempt from disclosure under the Privacy Act or FOIA because information may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

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

U.S. citizens and lawful permanent residents, as well as other persons with records covered by the JRA, are afforded the ability to correct information by filing a Privacy Act amendment request under the Privacy Act. U.S. citizens, lawful permanent residents, and persons covered by the JRA should submit requests to contest or amend information contained in FIRST. Individuals may direct all requests to contest or amend information to the USCIS FOIA/Privacy Act Office. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment Request." This would only apply to amendment of USCIS-held information. Persons not covered by the Privacy Act are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

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

USCIS notifies individuals of the procedures for correcting their information in applicable SORNs, this PIA, the Privacy Notices for Form G-639 and the Accounts Public account creation webpage, and through the USCIS website.[42] Specifically, the SORNs set forth in Section 1.2 and this PIA provide individuals with guidance regarding the procedures for correcting information. The Privacy Notices, including notice of an individual's right to correct information, are also contained on the instructions to Form G-639 and the Accounts Public account creation webpage.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk associated with redress. USCIS provides individuals with access to their records that are not subject to exemptions when requested through a FOIA or Privacy Act request. Individuals who are U.S. citizens or lawful permanent residents may submit a Privacy Act request to contest or amend information. Any person, regardless of immigration status, can come to a

[42] For more information, see https://www.uscis.gov/.

USCIS Field Office to update his or her records.

Section 8.0 Auditing and Accountability

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

USCIS ensures that practices in this PIA comply with federal, DHS, and USCIS policies and procedures, including privacy policies, standard operating procedures, orientation and training, rules of behavior, and auditing and accountability procedures. FIRST is maintained in the AWS, which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[43] AWS is FedRAMP-approved and authorized to host PII.[44] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. USCIS requires AWS to segregate FIRST data from all other third-party data.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls limit access to USCIS users and mitigate privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further, DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

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

All USCIS employees and contractors are required to complete annual privacy and computer security awareness training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements/Notices). The computer security awareness training examines appropriate technical, physical, and administrative control measures to safeguard information. USCIS employees and contractors within the FOIA Operations Division engage in professional trainings that cover a variety of topics related to privacy, including disclosure of information and safeguarding information. Additionally, FIRST users are required to

[43] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[44] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.

take role-based training.

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

Only FIRST System Administrators, Database Administrators, and select Subject Matter Experts from USCIS and ICE have direct access to FIRST. Access to FIRST is on a need-to-know basis. The need to know is determined by the individual's current job function. FIRST users are granted access following standard USCIS procedures for obtaining security clearances, active directory user identification names, and access to individual USCIS systems. FIRST users are assigned roles which limit access to data only as needed to fulfill their job functions.

FIRST system administrators and managers monitor FIRST to ensure only authorized users have access to information contained in FIRST. No guest accounts are ever created in FIRST. FIRST system administrators follow USCIS standard transfer and termination procedures to ensure that system accesses are revoked on employees or contractors who leave USCIS or are reassigned to other duties for which access is no longer required. FIRST managers review audit records for inappropriate activities in accordance with USCIS procedures. Downloading and the storage of PII outside of the FIRST system are not permitted. System administrators disable accounts when access is no longer needed.

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 has a formal review and approval process in place for new sharing agreements. Any new use of information and/or new access requests for the system must go through the USCIS change control process and must be approved by the proper authorities of this process, such as the DHS Headquarters (including Office of General Counsel, Civil Rights and Civil Liberties, Office of Intelligence and Analysis, and the Privacy Office), USCIS Privacy Officer, Chief of Information Security Officer, Office of the Chief Counsel, and the respective Program Office.

8.5 Privacy Impact Analysis: Related to the Accountability and Integrity of the Information.

Privacy Risk: The data maintained by AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS and are operated by a third-party vendor.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the FIRST system, whether on a USCIS infrastructure or on a vendor's infrastructure. Therefore, it

imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[45]

Privacy Risk: The documents maintained within the Digital Release Portal are vulnerable to a security and privacy breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is committed to protecting responsive documents in the Digital Release Portal against unauthorized access by employing strict technical and security controls. First, USCIS ensures FIRST, including the Digital Release Portal, operates in a secure environment. FIRST employs multiple layers of encryption to securely process all online transactions. Secondly, USCIS requires a two-factor authentication for account holders to access their accounts and the information that it contains. Two-factor authentication offers an additional layer of protection to ensure the security of online accounts beyond just a username and password. Lastly, account holders only have access to their information in the Digital Release Portal. All documents are linked to a unique online account number to ensure account holders are only able to assess responsive documents associated with a particular FOIA/PA request. The combination of these controls protect the information from unauthorized access. USCIS validates the implementation of its technical and security controls during the security authorization process.

Responsible Officials

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

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

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

[45] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.