Privacy Impact Assessment
for

RAILS

DHS/USCIS/PIA-075

November 5, 2018

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

Reviewing Official
Philip S. Kaplan
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 USCIS RAILS[1] Application System, which modernized and replaced the National File Tracking System (NFTS). RAILS is an automated file system that tracks internal immigrant files and receipt files, and allows for certain DHS users to request immigration files. RAILS enables USCIS to (1) electronically maintain an accurate file inventory, (2) track the location of paper and electronic immigration files via a web-based system and/or mobile application, and (3) allow users to order, transfer, and receive official paper and electronic immigration records related to the Alien Number (A-Number). USCIS is conducting this Privacy Impact Assessment (PIA) to analyze the privacy impacts associated with RAILS because RAILS collects, uses, and shares personally identifiable information (PII). The attached appendices discuss system interconnections. USCIS will update the appendices of the PIA when new USCIS, DHS, or external interconnected systems are added.

Overview

On March 1, 2003, U.S. Citizenship and Immigration Services (USCIS) assumed responsibility for the immigration service functions of the Federal Government. The Homeland Security Act of 2002[2] dismantled the Immigration and Naturalization Service (INS) and separated the agency into three components within the Department of Homeland Security (DHS). The law also formed U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) to oversee immigration enforcement and border security, respectively.

To support immigration benefit operations, USCIS and its partner components, ICE and CBP, create and use immigration files, especially the Alien File (A-File), in the course of performing their mission requirements. A-Files are created for individuals seeking immigration benefits (e.g., lawful permanent resident status, naturalization), individuals who illegally entered the United States, or other individuals subject to the provisions of the Immigration and Nationality Act (INA). The A-File contains official immigration records of persons who are not citizens or nationals of the United States, including records created as the individual passes through the U.S. immigration and inspection processes and, when applicable, records related to any law enforcement action against or involving the alien.

In addition to the A-File, USCIS and its predecessor, the legacy Immigration and Naturalization Service, created and used the following types of immigration files as a repository

[1] RAILS is not an acronym.
[2] Pub. L. No. 107–296, 116 Stat. 2135.

of various immigrant and non-immigrant benefit/application requests with a corresponding file number to associate an individual's immigration history with a unique record:

- Certificate Files (C-File) – Certificate files were created for persons naturalized prior to April 1, 1956.
- Non-Immigrant Files (N-File) – Non-Immigrant Files are older, temporary files that have mostly either been destroyed or consolidated with the A-File. These files related to limited time entry for temporary workers, trainees, or performers in the Arts.[3]
- Receipt Files – Receipt files are created for both immigrant and non-immigrant benefit applications. The receipt files for immigrants benefit applications will eventually be consolidated into an A-File;
- Substitute Files (S-File) – Substitute files are created when another file is required. The user must indicate that the file was lost or destroyed and then provide documents to support the Sub File creation.
- Temporary Files (T-File) – Temporary files are created to store documents when the A-File is in another office location. When the office receives the A-File, the documents within the T-File are merged with the A-File.
- Work Files (W-File) – Work files are created to place copies of original documents from the A-File. Work files are used for note taking and writing drafts. Drafts are then finalized and placed in the A-File.

As the custodian of the files listed above, USCIS is responsible for tracking the location of the more than seventy million existing immigration files described above. USCIS designated File Control Offices (FCO) serve as authorized offices that manage A-Files and Receipt Files throughout DHS, in the United States, and internationally. The Records Division, as part of the Immigration Records and Identity Services (IRIS) Directorate, has over 150 FCOs, including some that are co-located with CBP and ICE worldwide. FCOs include USCIS Headquarters, Field Office Directorate (FOD), Service Center Operations (SCOPS), Refugee Asylum International Operations (RAIO), ICE, and CBP. These offices can create, store, transfer, receive, and maintain A-Files. FCOs are also responsible for file retirements, mandatory physical annual audits of files, file consolidations, and for managing all file tracking and control reports. FCOs control all files in their jurisdictions, including files in sub-offices, field offices, Ports of Entry, and Border Patrol Stations within the surrounding area.

[3] The creation of N-Files stopped in the mid-1990s; however, there are residual N-Files in RAILS noting their location. These files do not appear in the Central Index System, and there is no need to request them. If an N-File is discovered, it is either consolidated with the individual's A-File or verified that the individual's status was temporary, and then destroyed accordingly.

To assist with tracking the location of immigration files throughout the FCOs, USCIS created the National File Tracking System (NFTS), a web-based application that allowed DHS to locate an immigration file within an office and track the movement of files between offices. As DHS moves to conduct immigration actions in an electronic environment, the paper immigration files are no longer the sole repository and official record of information related to an individual's official immigration record. DHS maintains immigration files in the following formats: (1) paper; (2) electronic; or (3) a combination of paper and electronic records. As such, USCIS used NFTS to reflect where a paper file was physically located, what USCIS case management system the electronic record resided in, or both. Through 16 years of modifications, updates, and additive requirements, NFTS has become a cumbersome, unreliable, and unsupportive system for the user community.

RAILS

USCIS is replacing the existing NFTS with a modernized version known as RAILS. USCIS will now rely on RAILS to be the automated file tracking system used to maintain an accurate file inventory and track the location of paper and electronic immigration files. This system facilitates DHS's ability to efficiently manage and streamline access to the millions of immigration files under its control. In order to accomplish this, RAILS interconnects with several systems, which are further described in the attached appendices. RAILS will use the same database and all file history from NFTS. When RAILS is completely operational, USCIS plans to decommission NFTS.

RAILS has introduced simplicity and improved the user experience by taking unnecessary, repetitive processes away from the users and automating them. An example of this is the reduction of 42 currently available user transactions in NFTS to 16 user transactions in RAILS. In addition, the system has been personalized to the individual user based on the user's approved role (basic user, records user, and administrator) and permission sets as assigned through MyAccess.[4] The inclusion of extensive back-end business rules has created an automated processing environment that will provide multiple checks and notifications to supervisors and records managers to help improve file accountability.

RAILS has been designed with the objectives of reducing the potential for misplaced and/or lost immigration files, simplifying the current processes, and providing an improved user experience. The following describes how the RAILS capabilities will help support those goals.

[4] The MyAccess application provides support for access to USCIS systems. MyAccess allows users to request access to USCIS systems, approve access requests, and review users for each system. MyAccess is currently configured to support USCIS, ICE, and CBP users for RAILS.

RAILS Dashboard

The Dashboard allows users to search for immigration files and see what tasks or immigration files are assigned to them. The Dashboard specifically displays the files that the user has requested, files that are in route to the user, and/or files that are assigned to the user. RAILS displays the total number of files for each category described and additional information regarding each file, such as the file number, applicant, date of birth, and country of birth.[5] From this Dashboard, the user can send, receive, request, audit, or search for immigration files. The user's alerts are also displayed on the Dashboard. Alerts may include newly requested, sent, and/or received files. This information can be displayed graphically too, meaning that the user can pull up pie charts showing the number of files in each status.

Inquiry File Details

This capability gives information regarding a specific immigration file. If the user also has access to the Central Index System 2 (CIS 2), RAILS shows the file number, the applicant's name, the applicant's date of birth, the applicant's country of birth, the status of the file, the current custodian of the file (an office name, not an individual's name), the last audit completed, if files were consolidated, if there are any rider files,[6] and the overall file history. RAILS receives and displays the applicant's biographical data through a new interface with CIS 2. However, this data is not stored in the RAILS database; it is simply being displayed in real time. When a user leaves the query screen, the data is no longer available.

File History

The history of the file is displayed on the same screen as the file details. It shows the tracking history of a file broken down by office location. The history includes the date of the transaction, the type of transaction (comment, received, sent, requested), the name of the employee associated with that file, the office location, and any comments made during the transaction.

Send Files

This capability allows users to send paper immigration files to other internal USCIS offices and to ICE and CBP when a file is requested. RAILS displays the total number of files in the send list, and RAILS also displays additional information regarding each file, such as the file number, applicant's name, and comment boxes to the user.[7] RAILS will alert the user if the user enters the

[5] This is done through an interface with the Central Index System. For more information, *see* Appendix A.
[6] Rider files are files that create or establish a relationship between two individuals. Examples of rider files include files on individuals involved in business fraud; files on family members that the services want to keep together so that the petitions are adjudicated together; or files related to enforcement needs for gang-related information that may need the alien numbers to stay together.
[7] Comment boxes can contain any additional information that a user wants to include. Comment boxes will typically include the file number, the FCO to which the file is being sent, the FCO that is sending the file, and location codes to identify the FCOs.

file number incorrectly or does not scan the file correctly. For example, if a file number is too long, too short, or does not exist in RAILS, then it will trigger an error message to the user. Once the user sends the files, the file status changes to "in-transit."

Receive Files

RAILS allows users to receive either a single paper immigration file or multiple paper immigration files from other internal and external organizations. This transaction moves files internally from one location to another.

Request Files

Users are able to request paper immigration files that are in the possession of another FCO. RAILS displays the file number, name of the subject of the file, and comment box(es) to the user. Users cannot request files that display the status "requested," "lost," "missing," and/or "in-transit." Once the user requests the files, the file status will automatically change to "in-transit." The process also allows users to cancel previously made requests.

Auditing

The FCO is required to conduct an audit of all files listed in an FCO's inventory at least annually, unless otherwise documented. RAILS allows users to audit their inventory to meet policy requirements. All files within a Responsible Party Code (RPC)[8] will be audited at the same time, not just an individual user's files. The audit function does not allow a user to change the file location. However, it will identify invalid file numbers, files not received by a RPC, remaining files unaudited for 14 days after a previous audit was initiated, and potentially missing files.

RAILS Supervisory Dashboard

In addition to the above features available to both users and supervisors, supervisors have a separate dashboard. The Supervisory Dashboard provides supervisors with real time visibility of key metrics of files for members of their team to better manage availability and accountability of immigration records. The Supervisory Dashboard displays graphs, which indicate the total number of aging files[9] and are broken down by number of days held at that location and their statuses. The Supervisory Dashboard also includes data overview charts showing Past Due Requests, files that have been "in-transit" for an extended period of time, missing files, and files unaudited that may have to be reported as missing.

[8] An RPC is a unique location code assigned to an individual or specific area within an FCO. It helps locate the exact location of a file within a facility/office.
[9] Aging files are the files located at a specific FCO and are broken down by the number of days the file has been held at that location.

File Tracking

RAILS has been developed to support the current hybrid records environment of paper and electronic immigration files while leaning towards a greater electronic file presence. When searching for an immigration file in RAILS, users will be presented with all official paper or electronic immigration files related to the A-Number.

RAILS is designed to track a file's movement between FCOs, within an FCO, and outside an FCO (e.g., when an employee takes files to an alternative work site).[10] When a user requires an A-File or other immigration-related record, the user goes into RAILS and requests the file. RAILS collects the following information directly from individual system users: system user's full name, office location, RPC, which relates to either a system user or file shelf location, the immigration file's status (e.g., archived, record-in-use[11]); and the last transaction (e.g., charged-out, received, in-transit). Any time a paper file is moved, the file is required to be scanned in or out using a RAILS scanning device for tracking purposes.

Each file is scanned using a scanning device for purposes of sending, retrieving, and auditing immigration files. There is a barcode on each immigration file folder, and users have Barcode Readers and Scanners to scan files in their possession within RAILS. Once the file is scanned, data is retrieved from the scanner and sent to RAILS for processing (i.e., updating the file's location).

RAILS transaction information is used to control the inventory of all files, query the file location, manage the request and transfer of files between offices and to/from the FCOs, provide reports to support management and cleanup efforts, and gather statistical information to improve the records processes. RAILS does not store a digitized copy or any content of the immigration files.[12] When the FCO receives the request for the paper A-File, the subject of the record's full name and primary tracking number associated with the file is printed on the pull ticket so that the FCO can verify the correct A-File is being pulled.[13] A request cannot be made for a file that is consolidated with another file, a missing file, a lost file, an in-transit file, a pre-requested file, an empty jacket file,[14] or any combination of statuses that cannot be requested. Electronic

[10] An alternative work site is a location where an employee performs officially assigned duties at home or other worksites geographically convenient to the residence of the employee and away from the traditional worksite. USCIS employees are permitted to remove USCIS files from the traditional worksite in accordance with the authorities listed in USCIS Management Directive No. 123-001.1.
[11] "Record In-Use" is a status used to alert users that would like to request a particular file that the file is needed at the assigned location for a designated amount of time.
[12] Digitized A-Files are maintained and stored in the Enterprise Document Management Service (EDMS). For more information, *see* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program, *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.
[13] Pull tickets are RAILS-generated lists of paper immigration files that have been requested to be sent to another FCO or a storage location.
[14] An empty jacket file is a preprinted folder that represents a valid Alien Registration Number.

immigration files also cannot be requested through RAILS as electronic files are located in another electronic case management system, such as Enterprise Document Management System (EDMS) or USCIS Electronic Immigration System (USCIS ELIS). However, RAILS would show in which system a particular electronic immigration file is located.

RAILS maintains and stores immigration file location information. RAILS also interfaces with the systems listed in the appendices at the end of this PIA, in real time, to either consolidate or share the latest status of the file location. Users of interconnected systems are able to view file location information that RAILS shares within that interconnected system.

RAILS MOBILE APPLICATION

The RAILS mobile application allows remote users, typically USCIS, ICE, or CBP personnel, to interact with RAILS through a mobile device. The RAILS mobile application allows ICE and CBP agents to record the transfer of documents in settings far from their respective office. These users are away from workstations for days at a time and lack the ability to process immigration file movement in the field.

The RAILS mobile application will allow USCIS, ICE, and CBP users to request or send files from a government device connected to a commercial cellular network. USCIS, ICE, and CBP employees will be using their government-issued phones to receive and send files from one FCO to another FCO, as well as within their office. Additionally, users are able to search for a file to find out its current location. The mobile application users will also have access to the same capabilities as RAILS, in terms of auditing, showing the history of a file, and inquiring the file.

Access to the mobile application will be limited to USCIS, ICE, and CBP users who are using a government-issued device. In order to access the mobile application, the user must have been granted access to RAILS. The user must log in to the RAILS web application to create a mobile device registration and set a mobile password. The web application will display a quick response (QR) code that the user must scan with the mobile application to complete the registration for that government-issued device. The user must use the registered government-issued device and know the password to log in to the RAILS mobile application.

Information sent or received by the RAILS mobile application is encrypted in transit via Hypertext Transfer Protocol Secure (HTTPS). The mobile application times out after 15 minutes of inactivity.

USCIS and CBP users use Airwatch to access the RAILS mobile application. Airwatch is a bridge between the mobile device and the USCIS network. Airwatch as a mobile device manager (MDM)[15] requires a mobile application to be installed on a device that USCIS wishes to manage.

[15] A mobile device manager contains software that allows IT administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

This application, Airwatch Agent, allows the device and the Airwatch MDM server to communicate. Once the Airwatch MDM application is installed and the user is authenticated, through a process known as device enrollment, the Airwatch Agent will help USCIS to control, manage, and secure the access to its network.

ICE users use the Blackberry MDM instead of Airwatch to access the RAILS mobile application. The users will authenticate with Blackberry in order to connect to the ICE network. The ICE and USCIS networks will allow network traffic to the RAILS mobile servers. Once ICE users authenticate with Blackberry and are able to reach the ICE network, they will also be able to access the mobile application.

The RAILS mobile application, in addition to providing file and receipt tracking information to USCIS, ICE, and CPB, has a long-term goal of having similar functions as RAILS. This mobile application will be further developed to include additional functionalities, at which time this PIA will be updated.

REPORTING

RAILS information is replicated in the Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR) for reporting, statistical analysis, and adjudicatory purposes. eCISCOR also connects with the Standard Management Analysis and Reporting Tool (SMART) to create customizable reports related to file tracking for other systems.[16] Each FCO is responsible for responding to, pulling, preparing, and sending A-files in accordance with the USCIS Records Policy Manual. RAILS allows each FCO to manually generate activity reports within RAILS identifying new tickets[17] and open tickets[18] that require action from the FCO. Each report includes the subject of the record's full name and the primary tracking number associated with the file (e.g. A-Number), along with the location of the sending office and the location to which the file is being sent. This information is necessary to identify pending tickets that have not yet been fulfilled and require USCIS action. As pull tickets are fulfilled, the records are removed from the reports during the next refresh.

[16] *See* DHS/USCIS/PIA-050 Standard Management Analysis Reporting Tool (SMART), *available at* https://www.dhs.gov/publication/dhsuscispia-050-standard-management-analysis-reporting-tool-smart.
[17] Each request generates a pull ticket that must be printed and placed in queue to be retrieved by FCO personnel. The New Tickets report show the file requests that have not been printed.
[18] Open Tickets are file requests that have been previously printed and not yet sent to the requestor. Note: once a file has been sent to the requestor, the ticket is closed and will no longer appear in Open Tickets.

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 Immigration and Nationality Act, 8 U.S.C. §§ 1101, 1103, 1304 et seq., and 1360 and the implementing regulations found in 8 CFR authorize the collection of the information contained in RAILS.

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

The information collected, used, maintained, and stored in both the RAILS system and the mobile application are covered under DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,[19] which accounts for documentation and maintenance of an individual's immigration application, petitions, and requests as he or she passes through the U.S. immigration process.

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

The full security plan for RAILS, is complete and under internal review.

RAILS has been granted an Authority to Operate and was accepted into the USCIS Ongoing Authorization program. Ongoing Authorization requires RAILS to be reviewed on a monthly basis and sustain its security and privacy posture in order to maintain its Authority to Operate.

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

The USCIS Records Division is coordinating with NARA to develop a record retention schedule for RAILS. The draft retention schedule will request the destruction or deletion of records within RAILS when no longer needed for agency business (e.g., short term retention (less than 10 years) for temporary records and 100 years from the date of birth of the subject of the record for permanent and or long-term temporary records).

[19] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).

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.

No. RAILS is not subject to the PRA requirements. RAILS, including the mobile application, only collects information directly from DHS federal employees requesting A-Files, and is therefore exempt from the PRA.

Section 2.0 Characterization of the Information

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

RAILS collects, maintains, uses, and shares information pertaining to the immigration file and the system user. RAILS will collect and maintain the following immigrant tracking numbers: A-Numbers, C-Numbers, Receipt Numbers, N-Numbers, T-Numbers, and W-Numbers that correspond with the file types outlined in the overview.

USCIS system interconnections allow RAILS to obtain information pertaining to the applicant, system user, and immigration file.

Applicant Data

RAILS maintains tracking numbers (i.e., immigration files numbers, such as A-Number, C-Number, Receipt Number, T-Number, and W-Number) that are used to retrieve transaction records related to the immigration file. Users are not able to view applicant's information beyond the tracking number.

However, if the user also has access to CIS 2, then through a new interface with CIS 2, RAILS can receive and display the applicant's biographical data when a record is queried in RAILS. When the user searches for a file in RAILS, the user can also see the applicant's biographical data, such as the name, date of birth, and country of birth. However, this data is not stored in the RAILS database, it is simply being displayed in real time. When a user leaves the query screen, the data is no longer available. The applicant's information will be visible in the background in order to verify that the correct record is being pulled from storage and sent to the requester in another USCIS office.

Immigration File Tracking Data

USCIS uses the immigration file tracking data to locate immigration related files within the custody of USCIS, ICE, CBP, and NARA. RAILS maintains the following data elements on the immigration files:

- FCO location;
- RPC;
- Status of the file (e.g., Archived, Records-In-Use, available electronically in EDMS or USCIS ELIS); and
- Last transaction (charge-out, received, in-transit) with a time stamp.

System User Data

USCIS uses the system user data to identify the user updating or querying RAILS. The system user would be a DHS employee or DHS contractor. RAILS maintains the following data elements:

- User ID;
- Last name;
- First name;
- Title;
- Email address; and
- Business phone number.

RAILS Mobile Application

The following information is what is passed to RAILS from the mobile application:

- Device ID and password entered by the user to authenticate;[20]
- Immigrant tracking numbers (e.g., A-Numbers, C-Numbers, Receipt Numbers, T-Numbers, and W-Numbers) entered by the user;
- Requests to send or receive files, including the immigrant tracking numbers entered by the user and any necessary supporting information provided by the RAILS system (e.g., the location where the file is being sent or from where it is being received); and
- FCO information entered by the user (e.g., office location).

[20] Although the mobile application stores the device ID and password, this information is not accessible to any RAILS users.

Using the inquiry feature in the RAILS mobile application, the information that is displayed to a user is limited to:

- FCO office, section, and RPC information;
- Immigrant tracking numbers entered by the user (e.g., A-Numbers, C-Numbers, Receipt Numbers, T-Numbers, and W-Numbers); and
- Related file numbers that may be relevant to the numbers already entered for the pending transaction (such as a Rider File).

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

RAILS collects and maintains limited immigration and naturalization information to ensure an accurate immigration file inventory and location information in support of the overall USCIS Records Management process. RAILS electronically interfaces and connects with NFTS,[21] CIS 2,[22] Global,[23] Computer Linked Application Management Information System (CLAIMS 3),[24] CLAIMS 4,[25] USCIS ELIS,[26] Customer Relationship Interface System (CRIS),[27] Immigrant Visa Content Service (IVCS),[28] eCISCOR,[29] and EDMS[30] to obtain limited information pertaining to the subject of the record, the system user, and the location of electronic and paper immigration files in order to track the current locations of immigration files. RAILS also connects with these systems to share the location and creation of paper and electronic immigration files. Generally,

[21] RAILS will interface with NFTS in order to migrate the data over to RAILS. NFTS will then be decommissioned.
[22] CIS 2 will eventually replace CIS. A PIA update for CIS 2 is pending. *See* DHS/USCIS/PIA-009(a) Central Index System (CIS), *available at* https://www.dhs.gov/publication/dhsuscispia-009-central-index-system.
[23] This system was formerly known as the Refugee, Asylum, and Parole System (RAPS). RAPS was decommissioned and replaced by Global. *See* DHS/USCIS/PIA-027(c) USCIS Asylum Division, *available at* https://www.dhs.gov/publication/dhsuscispia-027b-refugees-asylum-and-parole-system-and-asylum-pre-screening-system.
[24] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* https://www.dhs.gov/publication/dhsuscispia-016-computer-linked-application-information-management-system-claims-3-and.
[25] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4), *available at* https://www.dhs.gov/publication/dhsuscispia-015b-computer-linked-application-information-management-system-4-claims-4.
[26] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* https://www.dhs.gov/publication/dhsuscispia-056-uscis-electronic-immigration-system-uscis-elis.
[27] *See* DHS/USCIS/PIA-019 Customer Relationship Interface System (CRIS) Update, *available at* https://www.dhs.gov/publication/dhsuscispia-019b-customer-relationship-interface-system-cris.
[28] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.
[29] *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* https://www.dhs.gov/publication/dhs-uscis-pia-023a-enterprise-citizenship-and-immigrations-services-centralized.
[30] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.

most of the information in these source systems comes from the subject of the record when interacting with USCIS. See the attached appendices for a complete overview of system interconnections.

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 staff conduct audits of the physical location of files to validate the information in RAILS. USCIS policy requires at least one audit per year for each FCO. Most offices conduct rolling audits throughout the year. However, the National Records Center is required to be audited every five years.

On a daily basis, all offices manage RAILS reports for file accountability. Any file discrepancy, if found, is provided directly on the RAILS screen. If a file is found in an inaccurate location, then the user can reconcile the discrepancy by updating location information to the correct location. USCIS records users verify and correct the FCO contact information, as necessary, through RAILS. If after 14 days from the audit date an office has files whose location remains unreconciled, RAILS will flag the files as potentially missing to the records manager and supervisor for the applicable RPCs. This message states that there are files that remain unaudited and have not been moved to a Missing or Lost status. The Records Manager can get a list of files that are potentially missing through the Records Manager Dashboard.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that users may update RAILS with incorrect location information regarding FCOs and RPCs.

Mitigation: This risk is partially mitigated. The auditing procedures in place help to ensure the accuracy of the file locations. In addition, RAILS allows users to make edits to the file location directly in RAILS. Therefore, if a user has mistakenly entered an incorrect location, that location could then be edited and changed to the correct location. No one can make any changes to the image data for the electronic files.

Privacy Risk: RAILS receives information from multiple USCIS source systems. There is a risk that the information feeding into RAILS may be inaccurate.

Mitigation: This risk is partially mitigated. RAILS extracts data from numerous USCIS source systems and replicates the data elements in order to populate information about the subject of record, system user, and immigration file. However, USCIS has procedures in place to check the data accuracy of information coming into RAILS, including semi-annual audits of all FCO files. USCIS has the ability to correct inaccuracies brought to their attention by internal and public (via an amendment request) sources.

Privacy Risk: There is a risk of an over-collection of information or that information may be collected in RAILS that is not relevant.

Mitigation: USCIS mitigates this risk by maintaining only the minimal information that is necessary to verify the location of a paper or electronic immigration file. CIS 2 and other systems that interface with RAILS collect additional data from the subject of the record, but none of this information is maintained in RAILS.

Privacy Risk: There is a risk that USCIS may inadvertently disclose special protected class data (T, U, Violence Against Women Act (VAWA)) without a need-to-know.

Mitigation: This risk is mitigated because access to RAILS is limited to DHS employees. Confidentiality provisions outlined in 8 U.S.C. § 1367 authorize DHS (including USCIS, ICE, and CBP) to access and use Section 1367 information in support of their respective missions. Specifically, 8 U.S.C. § 1367(a)(2) provides that, with certain limited exceptions, the DHS is prohibited from disclosing any information relating to an individual who is the beneficiary of an application for T, U, or VAWA nonimmigrant status. This includes information about both principals and derivatives, and it covers any information about the individuals, including information provided to USCIS as well as the fact that he or she has applied for or received a benefit. The nondisclosure requirement does not apply to disclosures of protected information within DHS for legitimate agency purposes. Any DHS personnel who manage Section 1367 information, or may come in contact with this information, must receive the appropriate training for identifying and handling protective status cases. To mitigate the major privacy risk of unauthorized disclosure of information, and to protect the physical safety of the individual who filed the application or petition, USCIS requires the physical and electronic A-File to be appropriately marked to remind DHS personnel of the special handling policies and information sharing procedures relating to Section 1367 information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

RAILS is the primary system for providing immigration file location information for DHS. It supports DHS's need to track files at the local level, as well as nationally and internationally.

RAILS is designed to provide efficient access to high quality immigrant information by maintaining accurate file inventory and location information.

RAILS allows DHS to track the current locations of all immigration files being managed by USCIS, including archived files; to transfer files between FCOs and within a given FCO; to transfer files outside of FCOs (e.g., alternative worksites); to combine and consolidate files; and to audit the files in a given location. RAILS provides extensive reporting capabilities to track the files and an online historical query function. RAILS currently tracks approximately 139,000,000 files for over 24,000 users in 152 offices.

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?

Yes. USCIS provides certain authorized ICE and CBP personnel direct access to RAILS for the purpose of requesting, transferring, and receiving immigration files. RAILS has internal roles, through MyAccess, to control the access to different functions in RAILS. MyAccess controls and monitors system access in order to limit external access to those with a need-to-know. Roles are granted based on the user's business functions and are limited. For example, in order to send or receive immigration files, the user would have to be assigned the "send" and "receive" privilege within MyAccess. Each FCO has its own RAILS administrator(s). The administrator role has the permission to oversee the respective system location/FCO and gives employees within its designated FCO access to RAILS.

USCIS also provides ICE and CBP personnel access to RAILS through the RAILS mobile application. The RAILS mobile application allows a USCIS, ICE, or CBP employee to request, transfer, or receive immigration files even when he or she is working remotely (i.e., away from a workstation). In order to use the RAILS mobile application, the user needs to have an active user account in the RAILS web application and access to the DHS Application Store.

See below appendices for more information on interconnections with other DHS systems.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in RAILS may be used for purposes outside of the original purpose for which it was collected or that it may be disseminated inappropriately.

Mitigation: This risk is mitigated. To ensure the information is used in a manner consistent with the purposes of the original collection, USCIS monitors audit logs to ensure users are only accessing information related to their job functions. In addition, all users must be authenticated by Identity and Credentialing Access Management (ICAM) authentication. User privileges are governed by role assignments (e.g., non-records user, records user, and administrator). Prior to accessing RAILS, each DHS user must sign a user access agreement that outlines the appropriate rules of behavior tailored for RAILS. USCIS has established standard operating procedures that are also applicable to ICE and CBP and stipulate proscribed and permitted activities and uses, auditing requirements, and integrity controls.

USCIS implements disciplinary rules to ensure the appropriate use of the system. USCIS reminds employees accessing the system that the system may be monitored for improper use and illicit activity, and that penalties may apply for non-compliance, through a warning banner that reiterates the appropriate uses of the system. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This process acts as a deterrent to unauthorized activity.

Privacy Risk: There is a risk that unauthorized users may gain access to RAILS.

Mitigation: This risk is mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. RAILS is an application that is only available through the DHS USCIS network. All access is secured through access controls requiring ICAM authentication. Authorized employees must use their issued credentials, also known as Personal Identity Verification (PIV) cards, to gain access to RAILS. Individuals who do not require access to RAILS will not be able to access RAILS through their PIV card.

Privacy Risk: There is a risk that USCIS will be unable to track the location of a file if the file gets lost during transit.

Mitigation: This risk is mitigated. This risk is slightly outside the scope of RAILS as RAILS serves as a tracking and audit system. However, USCIS has put measures into place to protect files during transit. Files are shipped by United Parcel Service (UPS) or FedEx and are tracked in their respective systems with a tracking number. Files can also be shipped by United States Postal Service (USPS). If the FCO uses USPS to send files, the files must be sent by registered mail, which requires a signature upon receipt. Classified files are sent by USPS only in accordance with federal standard operating procedures for mailing and transmitting classified information. All files are sent with a manifest inside the package, and most offices will place a separate return notice with their address inside the box as well in case the package is somehow damaged.

Privacy Risk: There is a risk that USCIS will be unable to track the location of a file if an employee takes a file out of the workstation to the employee's telework location.

Mitigation: This risk is mitigated. In order to accommodate limited office space and flexible work schedules, USCIS has a robust telework program.[31] RAILS supports USCIS' telework program by tracking when an immigration file is moved between the government worksite and the telecommuting work site. If an employee needs to take a file to his or her telework or alternative workstation, the employee is required to scan each file removed using a RAILS scanning device. This is required when removing a file and returning a file to the FCO. Files cannot be sent to a telework or alternative workstation.

Privacy Risk: There is a risk that an employee will not scan the file when it is removed from the FCO, causing the record to become lost.

Mitigation: This risk is partially mitigated. As stated above, if an employee needs to take a file to his or her telework or alternative workstation, the employee is required to scan each file removed using a RAILS scanning device. This is required when removing a file and returning a file to the FCO. However, if an employee does not scan the file, then this could cause the record to be lost. There are auditing procedures at the individual user level and at the FCO level in place to help ensure the accuracy of the file locations.

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.

RAILS does not collect information directly from individuals. USCIS provides general notice to individuals through the Alien File, Index, and National File Tracking System SORN,[32] the associated source system SORNs (please see Appendices for a listing of the source systems), and this PIA. Furthermore, the instructions associated with each benefit request form contain a Privacy Notice. 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. Additionally, the forms

[31] Telework is any arrangement in which an employee performs officially assigned duties at home or other worksites geographically convenient to the residence of the employee and away from the traditional worksite. Employees who telework may be on a schedule from several days per week to as little as one day a month or on an as-needed basis for reasons, such as special projects, illness, weather disruptions, or unavailability of regular office hours.
[32] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).

also contain a provision by which an applicant authorizes USCIS to release any information received from the benefit requestor or beneficiary as needed to determine eligibility for benefits.

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

RAILS does not collect any new information directly from an immigration benefit applicant. The submission of a benefit request is voluntary. Individuals who apply for USCIS benefits are presented with a Privacy Notice and sign a release authorization on the benefit request. The Privacy Notice details the authority to collect the information requested. The forms also contain a provision by which a benefit requestor authorizes USCIS to release any information received from the benefit requestor as needed to determine eligibility for benefits In the law enforcement or national security contexts, notice or opportunity to consent would compromise the ability of the agencies to perform their respective missions; therefore, those systems are exempt from notice and consent provisions. Thus, for A-Files created for purposes other than immigration (e.g., enforcement, investigations), the individual does not consent to particular uses of the information. All PII in RAILS is extracted data from other systems as noted above.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk related to notice. The extent of notice and opportunity to provide consent vary based on the particular purpose associated with the original collection of the information in the systems of records from which the information is extracted. USCIS tailors the amount of PII used by RAILS to what is needed in a particular file tracking activity so that only the minimum PII necessary to perform the function is used. USCIS also provides notice through the Alien File, Index, and National File Tracking System SORN, any associated source system SORNs (please see Appendices for a listing of the source systems), and this PIA.

Section 5.0 Data Retention by the project

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

The draft retention schedule will request the destruction or deletion of records within RAILS when no longer needed for agency business (e.g., short-term retention (less than 10 years) for temporary records and 100 years from the date of birth for permanent and or long-term temporary records).

Although the actual A-File is not stored in RAILS (and the A-File has a separate retention schedule),[33] it is important to note that USCIS controls the subject's A-File for 100 years from the

[33] The A-File record retention schedule N1-566-08-11 was approved by NARA on March 30, 2009.

date of birth. When a file is selected to be archived, the file is digitized, and then transferred to NARA for permanent retention. RAILS continues to store the file location information even after an A-File is archived for accurate record-keeping purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that without an approved retention schedule, information may be retained longer than necessary, which may increase the potential of an unauthorized disclosure or deletion.

Mitigation: This risk is partially mitigated. USCIS is developing a retention schedule for RAILS and will not delete records until a retention schedule is approved by NARA. The proposed NARA schedule is consistent with the concept of retaining data only for as long as necessary to support the USCIS mission. Until a NARA-approved retention schedule for RAILS is complete, USCIS plans to maintain all records indefinitely in accordance with the Federal Records Act, which prohibits agencies from destroying records without a NARA-approved schedule.

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.

No. RAILS is not accessed outside of DHS at this time. USCIS plans to interface with external systems to provide the location of immigration records and will update this PIA prior to granting access to external entities.

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

No. RAILS is not accessed outside of DHS at this time.

6.3 Does the project place limitations on re-dissemination?

No. RAILS is not accessed outside of DHS at this time.

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

No. RAILS is not accessed outside of DHS at this time.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy impact related to external information sharing because RAILS is not accessed by entities external to the Department.

Section 7.0 Redress

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

An individual may seek access to his or her USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Account holders not covered by the Privacy Act or Judicial Redress Act (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. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

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 USCIS systems. Individuals may direct all requests to contest or amend information to the USCIS FOIA/PA 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." 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 this PIA, source system PIAs, Privacy Notices, and through the USCIS website.[34] Specifically, the SORN set forth in Section 1.2 provides individuals with guidance regarding the procedures for correcting information. This PIA also provides similar notice. The Privacy Notices, including notice of an individual's right to correct information, are also contained on the instructions to immigration forms published by USCIS.

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 United States 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 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 stated in this PIA comply with internal USCIS policies, including the USCIS privacy policies, standard operating procedures (SOP), orientation and training, rules of behavior, and auditing and accountability procedures. RAILS is maintained in the Amazon Web Services (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.[35] AWS is FedRAMP-approved and authorized to host PII.[36] FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

---

[34] For more information, *see* https://www.uscis.gov/.
[35] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[36] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.

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 controls limit access to USCIS users and mitigate privacy risks associated with unauthorized access and disclosure to non-USCIS users. 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 use auditing measures and technical safeguards to prevent 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. Additionally, RAILS users are required to 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 users with a need to know, such as RAILS System Administrators, Database Administrators, and users have direct access to RAILS. USCIS audits their access on an operating system level, as well as a database application level. If a user's account is expired or deleted, that user will not be able to log into RAILS. Users of interconnected systems cannot access RAILS directly through the interconnected system. Rather, users can view the file location information that RAILS has supplied to the interconnected system. All RAILS-connected systems have system logs that indicate details about conducted RAILS queries. These systems can also audit the list of registered users and each user's access permissions. Auditing does not include the ability to identify specific records each user can access, but audits can include the ability to identify the subject areas that each user accessed. Some systems conduct self-audits by reviewing logs, permissions, and access forms.

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 DHS Headquarters (including Office of the General Counsel, Office of 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 Amazon Web Services AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the RAILS system, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore 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.[37]

Responsible Officials

Donald K. 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]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

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

APPENDIX A: USCIS Systems Interconnections

- **NFTS:**[38] The legacy automated file-tracking system that was used to maintain an accurate file inventory and track the physical location of A-Files and is now being replaced with RAILS. RAILS has a direct connection to NFTS. USCIS plans to decommission and terminate the connection to NFTS once RAILS is fully operational.
- **Central Index System 2 (CIS 2**):[39] USCIS stores active and archived immigrant information in this system. CIS 2 includes tracking information on which FCOs have custody of immigrant files. RAILS processes file movement transactions within an office. RAILS provides CIS 2 with a mechanism for performing file requests and file location searches. Each transaction processing a file movement into or out of an office or Federal Records Center (FRC), operated by the National Archives and Records Administration, is reported to CIS 2 through the RAILS and CIS 2 interface. There are several transaction types: transfer in, transfer out, transfer forward, file retirement, file accession change, and FRC return. The interface with CIS 2 provides RAILS with biographical data. If the RAILS user is also a CIS 2 user, then RAILS pulls the name, date of birth, and country of birth for a specific A-File. The data is exchanged between the two systems through an encrypted connection. RAILS has a direct connection to CIS 2.
- **Global:**[40] Global is a case management system that supports the screening of individuals in the credible fear, reasonable fear, affirmative (I-589), defensive, and Nicaraguan Adjustment and Central American Relief Act (I-881) processes. It provides the means for tracking asylum cases as they progress from application filing through final determination/decision or referral to the U.S. Immigration Courts. RAILS maintains and controls the inventory of all A-Files, queries the file location, and manages the request and transfer of A-Files between Asylum Offices and FCOs. Global electronically inputs the A-Number and FCO into RAILS. RAILS provides file location information. RAILS has a direct connection to Global.

---

[38] RAILS will continue interfacing with NFTS until all necessary functionality is built in RAILS and NFTS is decommissioned. *See* DHS/USCIS/PIA-032 National File Tracking System (NFTS), *available at* https://www.dhs.gov/publication/national-file-tracking-system-nfts.

[39] CIS 2 will eventually replace CIS. A PIA update for CIS 2 is pending. *See* DHS/USCIS/PIA-009(a) Central Index System (CIS), *available at* https://www.dhs.gov/publication/dhsuscispia-009-central-index-system.

[40] This system was formerly known as the Refugee, Asylum, and Parole System (RAPS). RAPS was decommissioned and replaced by Global. *See* DHS/USCIS/PIA-027(c) USCIS Asylum Division, *available at* https://www.dhs.gov/publication/dhsuscispia-027b-refugees-asylum-and-parole-system-and-asylum-pre-screening-system.

- **Computer-Linked Application Management Information System (CLAIMS 3):**[41] CLAIMS 3 is the case management system that supports and maintains officer casework documentation and tracking for immigrant and non-immigrant benefit requests, with the exception of asylum and refugee related requests and applications for naturalization. CLAIMS 3 initiates the request by sending the Receipt Number to RAILS, and some fields are shared for generating report outputs. Report outputs include the Record Summary and the Transactions Completed reports. RAILS provides file location information through a direct connection with CLAIMS 3.
- **CLAIMS 4:**[42] CLAIMS 4 serves as the primary case management system for all naturalization applications. RAILS obtains the Receipt Number from this system, and some fields are shared for generating report outputs. Report outputs include the Record Summary and the Transactions Completed reports. RAILS provides file location information through a direct connection with CLAIMS 4.
- **Customer Relationship Interface System (CRIS):**[43] CRIS is a web-based system accessible through the USCIS website that provides customers with pending immigration benefit application case status information and estimated processing times. RAILS provides file location information through a direct connection with CRIS.
- **Enterprise Document Management System (EDMS):**[44] EDMS is a web-based system that allows users to search, retrieve, and view digitized A-Files and Receipt Files. USCIS scans the contents of an immigrant file and electronically stores the digital images in this system. When a file is digitized, EDMS sends updates to RAILS on a real time basis with the location of the digitized file, which allows RAILS to notify the RAILS user that the immigration file is electronically available in EDMS. RAILS has a direct connection to EDMS.
- **USCIS Electronic Immigration System (USCIS ELIS):**[45] USCIS ELIS is an electronic case management system that allows USCIS to process certain immigration

[41] *See* DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* https://www.dhs.gov/publication/dhsuscispia-016-computer-linked-application-information-management-system-claims-3-and.
[42] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4), *available at* https://www.dhs.gov/publication/dhsuscispia-015b-computer-linked-application-information-management-system-4-claims-4.
[43] *See* DHS/USCIS/PIA-019 Customer Relationship Interface System (CRIS) Update, *available at* https://www.dhs.gov/publication/dhsuscispia-019b-customer-relationship-interface-system-cris.
[44] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.
[45] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* https://www.dhs.gov/publication/dhsuscispia-056-uscis-

benefit requests. USCIS ELIS also maintains electronic A-Files. USCIS ELIS queries RAILS for file location and stores the current FCO location of the A-File in USCIS ELIS. USCIS ELIS sends a file transfer request to RAILS. USCIS ELIS sends the receipt number to RAILS. RAILS stores the USCIS ELIS receipt number, so RAILS users will know there is a case file in USCIS ELIS. RAILS has a direct connection to USCIS ELIS.

- **Immigrant Visa Content Service (IVCS):**[46] IVCS establishes an interface with the Department of State to intake digitized Immigration Visa petition forms and their supporting electronic documents in order to create electronic A-Files that will be stored in USCIS' EDMS. Once a digitized Receipt file is created or deleted in IVCS, the information is pushed to RAILS. RAILS provides file location information to IVCS. RAILS has a direct connection to IVCS, but does not share any information with the Department of State directly.
- **Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR):**[47] eCISCOR is a repository that contains copies of the systems discussed above and consolidates information collected during the adjudication of applications and petitions for immigration benefits. The USCIS RAILS/eCISCOR interface is used to track the file location information from RAILS and update it to the eCISCOR data store for use by interconnected systems. eCISCOR monitors changes in RAILS and pulls in changes in real time through a direct connection with RAILS.
- **Fraud Detection and National Security-Data System (FDNS-DS):**[48] FDNS-DS is the central repository for all data gathered during the processes of administrative investigation, background, identity, and security checks, and analysis of benefit fraud rates/trends. FDNS-DS allows FDNS Immigration Officers to cross-reference the background, identity, security check, and adjudicative process information for immigration applications and petitions with suspected or confirmed immigration fraud, public safety issues, and/or national security concerns. The RAILS/FDNS-DS interface is used for FDNS-DS to retrieve the physical locations of A-Files.

electronic-immigration-system-uscis-elis.

[46] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.

[47] *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* https://www.dhs.gov/publication/dhs-uscis-pia-023a-enterprise-citizenship-and-immigrations-services-centralized.

[48] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Directorate (FDNS), *available at* https://www.dhs.gov/publication/dhs-uscis-pia-013-01-fraud-detection-and-national-security-directorate.

APPENDIX B: DHS Systems Interconnections

At the publication of this PIA, there are no DHS interconnected systems to RAILS. USCIS will update Appendix B when new DHS interconnected systems are added.

APPENDIX C: External Systems Interconnections

At the publication of this PIA, there are no external interconnected systems to RAILS. USCIS will update Appendix C when new external interconnected systems are added.