Privacy Impact Assessment
for the

Integrated Digitization Document Management Program (IDDMP)

DHS/USCIS/PIA-003(a)

September 24, 2013

Contact Point
Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
(202) 272-8030

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

Abstract

The United States Citizenship and Immigration Services (USCIS) is republishing the previously published Privacy Impact Assessment (PIA) for the Integrated Digitization Document Management Program (IDDMP). IDDMP is the process of digitizing paper-based case files (A-Files and Receipt Files) and storing them in the Enterprise Document Management System (EDMS). EDMS enables the A-File to be shared more efficiently within the Department of Homeland Security (DHS) and with external agencies. USCIS is updating and reissuing this PIA to discuss in greater detail the IDDMP process in which information is ingested into EDMS.

Overview

The United States Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), is responsible for administering and processing applications for all immigrant and nonimmigrant benefits. To support immigration benefit operations, USCIS assembles a paper-based file, known as an Alien-File (A-File), which contains official immigration records of aliens or persons who are not citizens or nationals of the United States (U.S.) This function was previously the responsibility of the legacy Immigration and Naturalization Service (INS), which began issuing each alien an Alien Registration number (A-Number) in 1940, and on April 1, 1944, began using this number to create individual A-Files. A-Files contain all records of any active case of an alien not yet naturalized, including records created as he or she passes through the U.S. immigration and inspection process and, when applicable, records related to any law enforcement action against or involving the alien.

Since the formation of DHS in 2003, the U.S. immigration system has been managed by the following DHS components: 1) USCIS, which performs the immigration benefit adjudication process; 2) Customs and Border Protection (CBP), which performs the border enforcement and inspection processes; and 3) Immigration and Customs Enforcement (ICE), which performs the investigatory, deportation, and immigration court functions. Although USCIS is the custodian of the A-File, all three components create and use A-Files in the course of performing their mission requirements.

In addition to the management of A-Files by the DHS tri-components, the U.S. Department of State (DoS) also plays an important role in providing necessary immigration information to certain A-Files. DoS issues immigrant visas to individuals wishing to live permanently in the U.S.[1] In general, to apply for an immigrant visa, a foreign citizen must be sponsored by a U.S. citizen relative, U.S. Legal Permanent Resident (LPR), or by a prospective employer, and must be the beneficiary of an approved USCIS petition. Once USCIS approves the petition, it assigns the immigrant visa petition a Priority Date and sends the petition to the DoS National Visa Center (NVC). DoS NVC then manages the case and provides further instructions to the applicants, and collects and reviews required documents and evidence.

After DoS processes the visa, the visa recipient must indicate that he or she intends to adjust his or her status with USCIS. If he or she would like to pursue becoming an LPR, DoS sends USCIS all of

---

[1] A citizen of a foreign country who seeks to enter the U.S. generally must first obtain a U.S. visa, which is placed in the traveler's passport, a travel document issued by the traveler's country of citizenship.

the applicant information it collected as part of the visa process to be included in the A-File.[2] USCIS uses this information to determine if the applicant is eligible to adjust to a permanent resident.

Paper A-Files are currently under the control of the USCIS National Records Center (NRC) and the National Archives and Records Administration's (NARA) Kansas City Federal Record Center (KCFRC). However, USCIS, CBP, and ICE employees, who are stationed both domestically and internationally, require access to the A-File regularly to assist in adjudicating benefits, investigating immigration violations, and enforcing border protections. Because the A-File is inherently paper-based, sharing the physical file is expensive, prone to handling errors, and difficult to share within and across DHS components.

USCIS developed the Integrated Digitization Document Management Program (IDDMP) to manage the digitization of files and to provide electronic access to case files, including A-Files and Receipt Files, using the Enterprise Document Management System (EDMS).[3] IDDMP manages the process of scanning case files, which occurs at numerous capture facilities and including (1) Scan on Demand (SODA) at the NRC; (2) the USCIS Lockboxes; (3) the Records Digitization Facility (RDF); and (4) DoS. These capture facilities scan relevant case files and ingest them into EDMS through system interfaces. IDDMP also covers EDMS's ability to store, update, and access the electronic case file. Once scanned, the electronic version of the file becomes the official A-File and can be accessed by the tri-components using EDMS.

Enterprise Document Management System (EDMS)

EDMS is a web-based system that allows authorized users to view and search electronic copies of the paper-based case files: A-Files and Receipt Files. The tri-components require access to the information contained in these case files to learn the status of individuals, including permanent residents, naturalized citizens, border crossers, apprehended aliens, legalized aliens, aliens issued employment authorization, and other individuals of interest in order to successfully complete their job functions. EDMS permits quick and simultaneous access to case files 24 hours a day, 7 days a week.

Prior to the implementation of EDMS, USCIS manually provided case files to the tri-components in need of the file. If one of the tri-components requested a file, USCIS NRC staff queried the National File Tracking System (NFTS)[4] or the Central Index System (CIS)[5] for the physical location of the A-file, and would mail, fax, or email the case file to the requestor. Because this is a labor-intensive and time consuming process, USCIS sought out a more efficient means of sharing the file.

To alleviate this problem, USCIS developed EDMS to facilitate efficient information sharing. Tri-components requiring access to case files can now access the electronic file directly through EDMS,

---

[2] DoS may send the application, Affidavit of Support forms from sponsors, supplementary evidence, adjudicator notes, and any other information collected as part of the visa issuing process.

[3] EDMS also contains Receipt Files, which are files of immigrant and nonimmigrant benefit applications that USCIS receives. While the Receipt Files and supporting documentation are eventually consolidated into an A-File, EDMS allows users to view the immigrant and nonimmigrant applications electronically before receiving the official paper-based application. This allows USCIS adjudicators to begin processing cases in a quick and efficient manner.

[4] For a comprehensive explanation of NFTS, please refer to the DHS/USCIS/NFTS-032 PIA at www.dhs.gov/privacy.

[5] For a comprehensive explanation of CIS, please refer to the DHS/USCIS/CIS-009 PIA at www.dhs.gov/privacy.

which eliminates the paper-based process and reliance on physical case files. Additionally, the digitization of these files reduces the time for delivery from days to seconds and allows for multiple people to view the information at the same time.

There are two separate search functions in EDMS that users can search to locate either an A-File or Receipt File. Users can search EDMS to locate A-files and Receipt files using specific search criteria that allow the users to view the images in electronic format. Users can search A-Files in EDMS by either populating the A-Number, First Name, Middle Name, Last Name, Aliases, Date of Birth (DOB), Country of Birth (COB), Sex, Federal Employer Identification Number (FEIN), and Company Name fields. Users can search Receipt files in the same manner by using the Receipt Number that is assigned to the specific application, First Name, Last Name, A-Number, DOB, Accept/Reject Status, and/or Form Type.

The search capabilities within EDMS allow users to discover information that is buried deep within the physical A-File in a reduced time period through the use of metadata. Metadata are "tags" embedded into each document within the electronic case file for indexing and searching the digitized files. Metadata saved with every digitized A-File includes:

- First Name
- Last Name
- A-Number
- DOB
- COB
- Receipt Number

Although users cannot modify the digitized images within the file, EDMS enables users to locate information within the case file, add comments, modify documents contained within an A-File (dependent on a user role), and add additional documents to the file, through a process known as interfiling.

Furthermore, there are three digitization notification interfaces that allow EDMS to update the location in each system. EDMS provides real-time reporting via the EDMS web portal and deployed web services to track the status and errors related to ingestion. This ensures that the information in EDMS is accurate, complete, and up-to-date.

While only the tri-components have direct access to EDMS, contents in the digitized A-File are authorized to be shared with various external agencies pursuant to the routine uses outlined in the Alien File, Index, and National File Tracking System of Records Notice (SORN).[6] For example, when there is a valid business need, the A-File can be provided to federal, state, tribal, local, or foreign government agencies or organizations, or international organizations, responsible for providing benefits, investigating or prosecuting violations of civil or criminal laws, or protecting our national security.

---

[6] The DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records Notice (June 13, 2011, 76 FR 34233) is available at www.dhs.gov/privacy.

Case File Digitization Processes

IDDMP manages the scanning, receiving, storing, updating, and accessing of digital case files into EDMS. There are four processes that allow case files to be digitized and ingested into EDMS through system interfaces, including: (1) SODA; (2) the USCIS Lockbox; (3) the RDF; and (4) DoS. Tri-component employees can request that case files be digitized directly within EDMS or, if applicable, by contacting the capture facility in which the file is located. Once the employee sends the digitization request through EDMS, EDMS will locate the facility that maintains the file to begin the digitization processes. Each capture facility has an interface with EDMS to complete the automated ingestion of information into EDMS.

Scan on Demand (SODA)

SODA refers to the process of digitizing a paper-based A-file and making it available electronically upon receiving a request from a tri-component. The need to digitize an A-file is typically triggered by a submission by a tri-component that needs information contained in the file to assist in adjudicating a benefit application, initiating an enforcement action, or responding to a Freedom of Information Act (FOIA) or Privacy Act (PA) request. After USCIS receives a request, a USCIS NRC or NARA KCFRC employee will physically pull the requested paper files, digitize them, and make them available for the tri-components electronically in EDMS.

USCIS performs SODA for files located at the NRC or the NARA KCFRC. The NRC is the agency's primary record keeping facility that houses millions of immigration records in A-Files. NARA maintains USCIS records deposited with the National Archives of the United States at the NARA KCFRC.

The SODA digitization process involves three fundamental steps: (1) requesting a physical record; (2) producing the digitized records; and (3) delivering the digitized record.

Step 1: Requesting a record:

The requesting tri-component will submit a request for a file to be digitized within EDMS or by contacting the USCIS NRC Information Liaison Division (ILD) by email or phone; a person from the requesting component will generally provide the NRC with an A-Number or other identifying combination of personally identifiable information (PII), such as a name, country of birth, and date of birth of the individual whose A-file it wants digitized. ILD staff will log the request, including the A-Number and the requesting component personnel's contact information, into the SODA database.

ILD staff then use NFTS or CIS, the systems that track the location of A-files, to locate the physical paper A-file and include the location of the file in the SODA database. Once the ILD employee inputs the request into the SODA database, it is sent to another NRC employee for manual retrieval of the file.

Step 2: Producing the digitized record:

Once the A-file is located, the NRC staff will physically pull the file from the facility and convert the paper A-File into an electronic record.[7] NRC ILD staff use a scanner to scan files and then convert them to a format compatible with EDMS. NRC Quality Assurance (QA) staff reviews the digitized files to ensure they are identical and consistent with the paper file.

After the QA review, NRC staff uploads the scanned A-files into the capture facility to notify EDMS that the files are available. Once the notification has been received, EDMS retrieves the files via web services through the ingestion process. Once the NRC ingests the file into EDMS, all files are deleted from the scanner.

Step 3: Delivery of the digitized record:

Requests for files to be digitized are generally responded to within 15 days, depending on where the file is located. Once USCIS digitizes the file, it becomes the official immigration record.[8] Once EDMS ingests the A-File, it is searchable by the tri-component requester and any EDMS user.

The SODA database, which does not have a direct connection to EDMS, facilitates the digitization process, tracks pending requests, and compiles weekly, monthly, and yearly statistics related to the SODA process and administrative and system errors. NRC employees also use the database to manually record errors found during the government QA process and to track the correction of those errors.

USCIS Lockbox

In addition to A-Files, digitized Receipt Files from the USCIS Lockbox facility (Lockbox) that are scanned for initial intake processing are also ingested into EDMS.[9] Upon completion of a USCIS benefit application, USCIS instructs applicants to mail the form and any accompanying documentation to the appropriate Lockbox facility, which is found on the USCIS website and appropriate form. The Lockbox manages the intake of USCIS applications, petitions, and requests and the collection of associated fees submitted directly by mail. It provides the mechanisms to capture information electronically from USCIS applications, petitions, and requests; to deposit associated fees; to forward the

---

[7] In some cases, the requestor will only need one piece of information located in the A-File. If this is the case, ILD will pull that piece of information from the file and send only that information to the requestor by an encrypted email or secure fax.

[8] The electronic copy will become the official record pursuant to USCIS policy "Use of Digitized A-Files," dated March 28, 2008.

[9] The Lockbox facilities are operated by a financial agent authorized by the Department of Treasury. The financial agent is also responsible for preparing the files in accordance with USCIS guidance and sending the files to the next processing site. The financial agent does not approve or deny petitions/applications/requests received. USCIS has a business arrangement with the Department of the Treasury to allow Bank One, N.A. to serve as the USCIS financial agent. Bank One, N.A. provides USCIS lockbox imaging, check collection, and initial processing services. For more information regarding the Lockbox services provided by the Department of Treasury and appropriate financial agents, please see the Department of Treasury Electronic Check Processing PIA, available at http://www.fms.treas.gov/pia/ECP_PIA.pdf and the accompanying system of records notice, Treasury/FMS.017 - Collections Records -Treasury/Financial Management Service, May 15, 2009 (74 FR 23019) available at http://www.treasury.gov/FOIA/Pages/fmspa.aspx.

information to USCIS systems via an interface; and to generate receipt and rejection notices to individuals.

The Lockbox personnel review newly received filings to ensure they are properly filed. The Lockbox verifies the completion of the following items: basic biographical information, signature on the form, jurisdiction of the submitted form, correct fee, and basic eligibility of the individual. Once Lockbox personnel review the filings for accuracy, they convert the applications to electronic images called Receipt Files and upload them into EDMS.

The digitized Receipt Files are not considered the official USCIS record of the Receipt File and displays a watermark stating "COPY" on the electronic copy of the receipt file. The paper file remains the official record for the Agency. However, the Receipt Files are converted into an electronic format to research customer inquiries regarding accepted and rejected applications processed by the Lockbox, and to begin initial application review before the hardcopy is received from the Service Center.

The Lockbox provides document scanning and metadata capture to integrate with EDMS. Once the Receipt file is ingested into EDMS, it is searchable by any EDMS user. The Lockbox is searchable by receipt number because those temporary records are not yet A-Files. The Receipt File is eventually added to the A-file. A-Files in EDMS are searchable by A-Number, Name, Date of Birth, and Country of Birth. Once an A-number is assigned and the file is ingested into EDMS, the file become searchable by A-number and by the other metadata elements listed above.

Records Digitization Facility (RDF)

RDF provides physical and electronic records management, document scanning, metadata capture, and creation of information to integrate A-File images into EDMS. RDF is dedicated to providing its customers with timely access to complete and accurate information contained in the USCIS digitized files. Oversight of the RDF falls within the purview of the USCIS Headquarters Records Division, Program Management Office. The RDF process of ingesting files into EDMS is similar to SODA, except the files are not ingested upon request. Instead, the RDF is a multi-year plan to digitize approximately 1 million files per year and more than 70 million paper files over the course of several years. RDF staff use a scanner to scan files and then convert them to a format compatible with EDMS. RDF QA staff review the digitized files to ensure they are identical and consistent with the paper file.

After the QA review, RDF staff upload the scanned A-files into the capture facility to notify EDMS that the files are available. EDMS then retrieves the files via web services through the ingestion process once the notification has been received. Once the RDF ingests the file into EDMS, all files are deleted from the capture facility.

DoS Immigrant Visa Files

Previously, DoS shared this information with USCIS by sending USCIS the hardcopy forms and supplementary evidence. USCIS then stored this information in the applicant's paper A-File. As previously described, the sharing of paper-based A-Files is a labor-intensive and timely process. Digitizing files and storing them in a centralized system alleviates this process and allows USCIS to share information more efficiently.

DoS has agreed to create an electronic file of all the files sent back to USCIS, for eventual ingestion into EDMS. DoS has provided a server to USCIS containing a backlog of image files from USCIS applications and supporting materials of individuals on the DoS waiting list for a visa. Depending on the type of visa an individual is applying for, (e.g., immediate relative/family based, employment based and/or special immigrant) there may be a numerical limit of visas granted each year, and wait times may be involved. Wait times can vary, are dependent on the applicant's country of citizenship, and can be very lengthy. Visa processing will not occur until the NVC contacts the applicant and tells him or her that the wait time is complete.

Once DoS approves the applicant's visa and the applicant determines he or she would like to adjust his or her status with USCIS, USCIS will assign the individual an A-number. At this point, USCIS will retrieve the applicant's information from the server and ingest the information into EDMS. No information will be ingested into EDMS until the applicant is assigned an A-number. If the visa is denied, or the applicant does not contact USCIS to adjust his or her status, the information will remain on the server. The information contained on the servers cannot be retrieved or accessed by anyone other than the server administrators. Once the individual is assigned an A-Number and his or her information is put into EDMS, the information will be accessible by all EDMS users.

The above section describes all of the processes for ways in which information can be ingested into EDMS for efficient sharing throughout the DHS tri-components. USCIS is republishing this PIA because the previous PIA did not distinguish the different processes and sources for how information is ingested into EDMS. By reissuing the PIA, we hope to fully address the privacy issues associated with IDDMP and show each piece of the process. If additional process or users of EDMS are added in the future, USCIS will update this PIA.

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 specific legal authority for this collection of information is Section 290(a) of the Immigration and Nationality Act. Additionally, per Office of Management and Budget (OMB) Memorandum M-12-18, "Managing Government Records Directive," by 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format.[10]

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

The SORN that covers this collection of information is the Alien File, Index, and National File Tracking SORN, June 13, 2011, 76 FR 34233.

---

[10] The OMB Directive can be found at www.whitehouse.gov/omb.

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

EDMS was approved for operation on July 30, 2012, for a period of 18 months. The Authority to Operate (ATO) is set to expire on January 31, 2014. The EDMS Security Plan was completed in March 2012.

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

NARA approved the EDMS N1-566-08-17 retention schedule. Additionally, the files sent to USCIS by DoS are covered by the N1-566-12-03 retention schedule. USCIS retains A-Files and Receipt Files in accordance with N1-566-08-11 and N1-85-96-01, respectively. N1-GRS-95-2 item 1c, governs the SODA Database, which allows records to be deleted/destroyed when no longer needed for administrative, legal, audit, or other operational purposes.

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.

IDDMP does not collect information directly from an individual and there are no forms associated with this collection. The IDDMP maintains data from USCIS applications and petitions that are covered by the PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

<u>A-File</u>

IDDMP does not collect information not already collected through an existing process. IDDMP digitizes hard copy A-Files so they may be shared more efficiently throughout DHS in support of benefit application, enforcement action, or receipt of a FOIA/PA request.

The A-File contains information including, but not limited to:

- First, Middle, and Last Name;
- Alias(es);
- Sex;
- Address;
- Telephone Number;

- Social Security Number (SSN);
- A-Number;
- Passport Number;
- DOB;
- COB;
- Country of Citizenship (COC);
- Vital documents (e.g., birth certificates, passports, marriage certificates);
- Biometric information (e.g., photographs, fingerprints);
- Enforcement supporting documents (e.g., rap sheets); and
- Other documents (e.g., naturalization certificates; tax returns; labor certifications; correspondence; court dispositions; interview notes).

A-Files sometimes contain media that cannot be scanned, such as videotapes, audiotapes, and CDs. The contents of such media will not be included in the digitized A-File, but the digitized A-File will note its presence in the physical file.

Receipt File

The digitized Receipt File contains but is not limited to:

- First and Last Name;
- Alias(es);
- Sex;
- Address;
- Telephone Number;
- SSN;
- A-Number;
- Passport Number;
- DOB;
- COB;
- COC; and
- Any other information collected on the associated form.

SODA Database

The SODA database collects and stores the following information:

- Employee/Requestor Name;

- ILD Employee User ID;

- Name of requesting agency;

- A-Number; and

- File location.

The metadata saved in EDMS with every digitized A-File includes:

- A-Number;

- First Name;

- Last Name;

- DOB;

- COB; and

- Receipt Number.

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

IDDMP does not collect data directly from an individual. The information contained in EDMS is generally collected from an individual or representative seeking an immigration benefit or has some encounter with the U.S. immigration system. The employee data contained in the SODA database is collected directly from the DHS employee requesting the information.

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

IDDMP does not collect information from commercial or publicly available data sources.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data in EDMS is dependent upon the accuracy of the information in the paper A-File and/or Receipt File. USCIS collects information contained in these files directly from the individual or his or her representative. The A-File may also contain information that was input into the file from tri-components or DoS during the course of providing benefits, investigating or prosecuting violations, or protecting our nation.

Additionally, QA personnel perform extensive quality monitoring and assurance reviews throughout the digitization process to ensure that the paper case files are scanned into legible and accurately identified digitized files. Pages are checked to ensure that they are fully rendered; properly aligned and ordered; free of distortions; and named correctly. Metadata entered at scanning operations undergoes similarly rigid quality control checks. QA personnel will identify, review, correct, and log inaccuracies to prevent recurrence.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The information contained in the case file may be inaccurate or incomplete.

Mitigation: The digitized file in EDMS may not include all material that exists for the paper case files. If there is material within the A-File that cannot be digitized, i.e., video tapes, USCIS employees will annotate in EDMS that one or more of documents in the original could not be scanned. USCIS creates Temporary Files (T-File) to store permanent documents, when the original A-file is not available. USCIS employees conduct searches in NFTS to determine if there are existing T-Files available. Lastly, if errors are found in a digitized case file, the facility that digitized the file receives notice and the facility employees review the electronic and physical file to correct the error. Furthermore, QA personnel perform quality monitoring and assurance reviews throughout the digitization process and can identify, review, correct, and log inaccuracies to prevent recurrence.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

The uses of the information contained in EDMS are the same as the uses for the paper A-file and Receipt File. The information is used for immigration benefits processing, law enforcement, and protection of national security. Specific uses of these case files are to:

- Confirm identity using dates of birth, photos, or other biographic or biometric information;

- Confirm relationships using information found in birth, marriage, divorce, and/or adoption certificates;

- Confirm law enforcement actions using investigation reports, rap sheets, etc.;

- Confirm previous immigration benefit processing, including both approvals and denials; and

- Research customer inquiries and begin initial application review.

Storing case file information electronically in EDMS allows DHS, in the standard course of its immigration-related business to: access the files more rapidly and efficiently, concurrently and collaboratively use the files, and mitigate the risk of losing the paper-based files. EDMS eliminates the inefficiencies associated with paper records, such as slow, resource-intensive shipping, high risk of loss, and deterioration over time.

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.

IDDMP does not use technology to conduct electronic search, queries, or analyses to discover or locate a predictive pattern or an anomaly.

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

The A-File, on paper or as digitized as part of IDDMP, is the record that contains all transactions involving an individual as he or she passes through the U.S. immigration and inspection process, and chronicles interactions with the U.S. Government. These functions have been divided among USCIS, CBP, and ICE. Although USCIS is the custodian of the A-File, all three components create and use A-Files.

Once an A-File is digitized, information is accessible by all three components so that they may perform their respective mission requirements. Information contained within the A-File may also be shared with other components within DHS responsible for law enforcement activities and protection of national security. In addition, access may be granted to the DHS Office of the Inspector General, primarily for the purpose of conducting internal investigations and evaluations of DHS employees conduct in the performance of their duties. Information is also shared in order to support associated management reporting, planning and analysis, or other administrative uses that require access to the information contained in the A-File.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Individuals who have legitimate access to PII could exceed their authority and use the data for unofficial purposes.

Mitigation: USCIS strictly manages access controls and policies; auditing; and other physical, technical, and administrative controls. USCIS limits the use and access of all data to purposes for which it was collected. Only employees who need access to the A-File to perform their official duties are granted access to EDMS. System users must complete mandatory Computer Security Awareness training, Privacy training, and EDMS training. USCIS employees who take requests to digitize case files and who digitize the files themselves have additional training on the process. All contractors must sign non-disclosure agreements. Data must always be securely transferred. For example, if EDMS data is transferred on portable media or via email to authorized DHS employees, National Institute of Standards and Technology (NIST)-approved encryption is used to ensure that data is not tampered with en route and to prevent unauthorized personnel from viewing it.

Section 4.0 Notice

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

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

IDDMP does not collect information directly from an individual. Instead, it scans paper-based information originally provided to DHS by an applicant and stores the digitized A-Files in EDMS. All individuals applying for a benefit are presented with a Privacy Act Statement that informs the individuals of the purpose and authority for collection, routine uses of the information, and if the submission of

information is voluntary or mandatory. Individuals also receive general notice through the publication of this PIA and the Alien File, Index, and National File Tracking System of Records Notice (SORN), June 13, 2011, 76 FR 34233.

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

IDDMP does not collect information directly from an individual. Information is collected by various means and stored in EDMS as a digitized version of the paper A-File. Applicants who seek USCIS benefits receive a Privacy Act Statement, which details the authority and uses of information. When submitting the application, the applicant certifies and authorizes the release of any information to appropriate agencies in accordance with the approved Routine Uses outlined in the applicable SORN. USCIS informs the applicant at the point of data collection (generally on the form itself) that it is within his or her rights to decline to provide the required information; however, it will result in the denial of the benefit request.

4.3   Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk of insufficient notice describing the purpose, use, and effects on the requestor for failing to provide information.

Mitigation: USCIS mitigates this risk by providing notice to the individual prior to the collection of information through the inclusion of a Privacy Act Statement on each form, the publication of this PIA, and other relevant PIAs such as NFTS and CIS, on www.dhs.gov/privacy, and the publication of the A-File SORN in the Federal Register.

Section 5.0 Data Retention by the project

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

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

The A-File is the record that contains all transactions involving an individual as he or she passes through the U.S. immigration and inspection process. A-File records are permanent records in both electronic and paper form. USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.[11] When USCIS digitizes a paper A-File, the digitized A-File maintained in EDMS becomes the official record and maintains the same retention schedule as the original paper A-File. Once USCIS digitizes the files, it sends the paper-based files to NARA or the KCFRC.

Contrary to the digitized A-File, digitized Receipt Files are copies and not the official Agency record of the Receipt File. The paper file remains as the official record for the Agency.

5.2   Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that USCIS may retain information longer than is necessary to approve or deny the benefit sought.

---

[11] Newly-eligible files are transferred to the KCFRC every five years.

Mitigation: USCIS retains data beyond the approval or denial of a benefit in order to ensure the information is available for several purposes, including future immigration status verification, evaluating subsequent benefits sought by an applicant, and for litigation. The digitized A-File serve the same purpose as the paper-based A-File, which NARA has determined to be of permanent historical value. When information is no longer necessary, USCIS retires the records according to the retention schedules listed in section 1.4 of this PIA.

Section 6.0 Information Sharing

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

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Upon request, copies of a digitized A-File or certain documents within an A-File can be made available to external agencies that do not currently have access to EDMS but have a valid need for the immigration record. Encrypted PDF images from EDMS can be exported to CD for distribution through postal mail or, alternatively, digitized A-File documents can be compressed and sent via e-mail as an encrypted attachment. In special circumstances, such as national security events, the original physical A-File might be requested. If the need for the original physical A-File is valid, the paper file will be pulled from retired status and sent to the requesting agency. The digitized version of the A-File will no longer be available in EDMS in such instances.

Information in the digitized A-File may be shared with external organizations for the purpose of providing benefits, law enforcement, or other uses consistent with the routine uses described in Alien File, Index, and National File Tracking System of SORN, June 13, 2011, 76 FR 34233. Furthermore, information may be shared with Department of Justice to assist in the development of agency's legal and/or policy position and Department of State in processing of petitions or applications for benefit under the Immigration Nationality Act. If external agencies receive direct access to EDMS in the future, USCIS will update this PIA.

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

USCIS only shares information outside of DHS as permitted under the Routine Uses outlined in the Alien File, Index, and National File Tracking System of SORN, June 13, 2011, 76 FR 34233 SORN.

6.3 Does the project place limitations on re-dissemination?

Prior to disclosing any information to an external agency, DHS must have a Memorandum of Understanding (MOU) in place with the partner agency fully outlining responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination. Methods and controls over dissemination of information are coordinated between DHS the partner agency, prior to information sharing. Depending on the context of other sharing, DHS may place additional controls on the re-

dissemination of the information.

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

Pursuant to 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 as a routine use pursuant to 5 U.S.C. 552a(b)(3).

For any external sharing, USCIS requires a representative from the outside agency to establish, in writing, what specific information it needs about particular individuals and ensures that it is consistent with the Routine Uses listed in the SORN. This is process is begins when the requesting agency completes the G-658 *Record of Information Disclosure (Privacy Act).* This form is used to record the reason for each disclosure and is maintained in the Subject's A-File or maintained in such a way that it can be easily retrieved when requested.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that USCIS may share data outside of DHS for purposes that are not in accordance with the stated purpose and use of the original collection.

Mitigation: USCIS is careful to only share data with external agencies that have a need-to-know and will use the information in a way that is compatible with the original purpose for collection described in the A-File SORN. All external sharing arrangements are reviewed prior to the sharing of information to ensure such uses are consistent with existing published routine uses in the applicable SORNs and/or performed with the consent of the individual whose information is being shared. The Privacy Act Statement included on USCIS Forms notifies the individual that USCIS may provide information from the form to other government agencies. As required by DHS procedures and policies, all current external sharing arrangements are consistent with the original purpose for which the information was collected.

Section 7.0 Redress

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

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

An individual may gain access to his or her USCIS records by filing a FOIA/PA request. Any individual seeking access to his or her USCIS record may submit the aforementioned requests to following address:

National Records Center

Freedom of Information Act/Privacy Act Program

P. O. Box 648010

Lee's Summit, MO 64064-8010

The information requested may, however, be exempt from disclosure under the Privacy Act because sometimes files contain law enforcement sensitive information and the release of could possibly compromise ongoing criminal investigations. Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

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

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Individuals may direct all requests to contest or amend information to the FOIA/PA Office at USCIS at the address listed above. They must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment thereof.

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

The procedures for individuals to amend their information are outlined in this PIA and Alien File, Index, and National File Tracking SORN, June 13, 2011, 76 FR 34233.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that an individual's opportunity for redress may be limited by a Privacy Act exemption.

Mitigation: Individuals are given numerous opportunities during and after the completion of the application process to correct information they have provided and to respond to information received from other sources.

Section 8.0 Auditing and Accountability

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

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

DHS security specifications require USCIS to maintain audit logs that document the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. In accordance with DHS security guidelines, USCIS systems use auditing capabilities that log user activity. All user actions are tracked via audit logs to identify audit 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. USCIS systems have internal audits separate from the domain security audits; therefore, a double layer of audit trails exists. Furthermore, each employee is required to undergo annual security awareness training that addresses his or her duties and responsibilities to protect the data.

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

USCIS provides annual privacy and security awareness training to all employees and contractors. The Culture of Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations. The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls that safeguard information. Lastly, all users are required to complete EDMS training prior to being granted access to the system.

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

EDMS has three types of users: general users, records administrators, and system administrators. The permissions available at each level are outlined below. The user's type will be identified at login, authenticated through the DHS Active Directory instance, and the user will be assigned the correct access rights.

- General users have the ability to perform A-Number, metadata, and full-text searches, and view documents.
- Records administrators have the ability to view the documents for A-Files, can edit the metadata for A-Files and their associated documents, and view reports on auditing and ingestion.
- System administrators have the ability to view the metadata and documents for A-Files and can delete them.

Functions	General Users	Records Admin	System Admin
Logging In	X	X	X
A-Number / Account / Receipt File Number Search	X	X	X
Expanded Search	X	X	X
Search Results	X	X	X
Search within an A-File	X	X	X
View/Print A-File Documents (Watermarked)	X	X	X
View A-File Documents (Non-Watermarked)		X	X
Print A-File Documents (Non-Watermarked)		X	X
View/Print Account Documents (Non- watermarked)	X	X	X
Export A-Files		X	X
Create Certified Printed copy of an A-File		X	X
Edit Comments			X

Delete Comments			X
Delete Documents			X
Delete A-Files			X
Edit Receipt File Retention Period (Apply/Remove Hold)		X	X
Add descriptive text to A-File documents	X	X	X

USCIS deploys role-based access controls and enforces a separation of duties throughout the lifecycle of the electronic A-File. Access is limited to only those persons who have a need-to-know in order to perform their duties. This need-to-know is determined by the respective responsibilities of the employee.

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 formal review and approval process in place for new sharing agreements. Any new use of information and/or new access requests for USCIS systems must go through the USCIS change control process and must be approved by the proper authorities prior to sharing information within and outside of DHS.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

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