# Privacy Impact Assessment

**for the**

# Administrative Appeals Office Case Management System

**DHS Reference No. DHS/USCIS/PIA-062(a)**

**January 30, 2023**

Homeland Security

# Abstract

The U.S. Department of Homeland (DHS) U.S. Citizenship and Immigration Services (USCIS) Administrative Appeals Office (AAO) uses the AAO Case Management System (CMS) to capture and track information related to appeals, motions, and certifications that AAO adjudicates under its jurisdiction, and to improve its ability to track appeals and case processing. USCIS is conducting this Privacy Impact Assessment (PIA) update to account for the capture of additional information in the AAO Case Management System, as well as to identify the privacy risks and mitigations associated with the collection and use of that additional information.

# Overview

The USCIS AAO developed the AAO Case Management System to track adjudicative work performed by AAO using the Salesforce Government Cloud.[1] The Salesforce Government Cloud provides a trusted and secure service to the U.S. Government, and quickly and securely delivers applications to meet customer's needs. Customers are able to create business applications by tailoring applications built by salesforce.com (Service Cloud, Sales Cloud) or by building their own custom application on the Salesforce platform. The AAO Case Management System is used to track appeals, motions, and certifications filed with or processed by USCIS AAO.

All incoming appeals, motions, and certifications are initially received, accepted, and entered by the Lockbox[2] or Service Center[3] into Computer Linked Application Information Management System 3 (CLAIMS 3)[4] and USCIS Electronic Immigration System (USCIS ELIS)[5] for processing. CLAIMS 3 and ELIS are the official systems of record for dates and actions on appeals, motions, and certifications and display basic information about each application or

[1] The Salesforce Tracking Activities and Relationship System (STARS) is a USCIS major application hosted in the Salesforce Government Cloud Software as a Service (SaaS) solution to securely deliver applications to meet USCIS needs. The AAO built its case management system using the Salesforce Government Cloud. The purpose of the Salesforce Government Cloud is to provide a trusted and secure service to the U.S. government to quickly deliver applications to meet customers' business needs.

[2] Lockboxes are facilities where individuals mail their paper forms. Once received by the Lockbox, USCIS staff scan the forms/complete manual data entry to upload the form information into the correct USCIS system. For more information on the Lockbox processes, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE BENEFIT REQUEST INTAKE PROCESS, DHS/USCIS/PIA-061, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[3] In early April 2021, many Notice of Appeal or Motion (Form I-290B) receipts began to be receipted, accepted, and ingested into USCIS ELIS by the Lockbox. For a period of time, Service Centers will continue to receipt into CLAIMS 3; however, eventually all Form I-290Bs will be receipted into ELIS.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3), DHS/USCIS/PIA-016(a), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZEN AND IMMIGRATION SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS), DHS/USCIS PIA-056, *available at,* https://www.dhs.gov/uscis-pias-and-sorns.

petition. Though the official events are recorded in CLAIMS 3 and ELIS, they are not designed as case management systems for the appellate work the AAO performs. The AAO lacked a system by which to track receipts, assignments of work to officers, adjudications, or administrative actions for its work. Consequently, leadership at the AAO lacked the necessary visibility into workloads to respond in a timely manner to workload spikes, understand trends, and efficiently report on results. Thus, the AAO Case Management System was built.

## Reason for the PIA Update

USCIS is updating the AAO Case Management System Privacy Impact Assessment to include additional biographic information from the Form I-290B, *Notice of Appeal or Motion,* and background check and security information AAO officers collect during security and fraud referrals related to appeals, motions, and certifications.

**Form I-290B*, Notice of Appeal or Motion***

Form I-290B requests information about the applicant/petitioner and information about the appeal/motion. Form I-290B also requests information regarding the basis of the appeal or motion request, the USCIS form under appeal or motion, the date of adverse decision, and the office that issued the adverse decision.

Individuals or representatives mail forms, supporting documents, and the applicable fee payment or waiver to either a USCIS Service Center or USCIS Lockbox facility based on his or her region and the type of benefit request appealed.[6] Individuals or representatives file the appeal form according to the specific instructions provided on Form I-290B or the denial notice.

Incoming paper-based forms are received and reviewed by USCIS personnel at a Service Center or Lockbox facility. USCIS personnel review the benefit request form and supporting evidence for completeness. Every form must include complete information in all required blocks, be signed, and— unless the fee is waived—include the correct fee. The information from the Form I-290B is entered into CLAIMS 3 or ELIS to establish the authoritative USCIS electronic record regarding the appeal. The AAO uses the information the applicant/petitioner provides on the Form I-290B to adjudicate appeals or motions on decisions under the Immigration and Nationality Act (INA), as amended.

Form I-290B collects information about the applicant, petitioner, beneficiary, derivatives, and household members and information about the appeal/motion. Information collected about the applicant/petitioner includes the following:

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE BENEFIT REQUEST INTAKE PROCESS, DHS/USCIS/PIA-061, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

- Full name;
- A-Number;
- USCIS Online Account Number;
- Receipt Number;
- Mailing address;
- Daytime telephone number;
- Mobile telephone number;
- Email address;
- Attorney or accredited representative name; and
- Signature.

Form I-290B also requests information regarding the basis of the appeal or motion request, USCIS form under appeal or motion, date of adverse decision, and the office that issued the adverse decision. USCIS updated the Form I-290B to include the following additional data elements:

- Date of birth of the individual filing the Appeal or Motion; and
- An alternate or safe mailing address for Violence Against Women Act (VAWA), Victims of Trafficking and Violence Prevention Act of 2000 (T and U), and Special Immigrant Juvenile Cases.

The AAO Case Management System contains data from Form I-290B as maintained in CLAIMS 3[7] or ELIS.[8]

**Background Check and Security Information**

AAO traditionally conducts background security checks, in accordance with the National Background, Identity, and Security Check Operating Procedures policy, developed by the Fraud Detection and National Security Directorate (FDNS), which sets the standard for USCIS security checks. These background checks and other fraud detection and national security efforts are currently tracked on paper and filed according to the Records Policy Manual (RPM).[9] As appeals

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3), DHS/USCIS/PIA-016(a), available at https://www.dhs.gov/uscis-pias-and-sorns.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS), DHS/USCIS/PIA-056(a), available at https://www.dhs.gov/uscis-pias-and-sorns.
[9] For additional information see: Records Policy Manual, *available at* https://connect.uscis.dhs.gov/org/IRIS/IIMD/RPM/Pages/rpm_default.aspx.

and motions transition to electronic processing, there is a need to collect and track such information within the AAO Case Management System to streamline communications between officers, supervisors, and the AAO FDNS team. AAO plans to begin processing and documenting these background checks (and any future required background checks) in the AAO Case Management System.

Background checks are critical to maintaining the security and integrity of the United States immigration system as they include, but are not limited to, examination of law enforcement systems such as CBP TECS[10] and Customer Profile Management System (CPMS)[11] Federal Bureau Investigation (FBI) fingerprint results, as well as site visits coordinated with other DHS and local law enforcement entities. Currently, such checks are documented in the paper file, which makes access by the officers and supervisors in the AAO's current workforce environment challenging. By documenting the results in the AAO Case Management System, a greater level of efficiency will be achieved, as possession of the physical file will no longer be needed to access such results. The privacy and security of any information contained in the AAO Case Management System will be protected to the same extent in which it is protected within a physical file. Only the AAO has access to this Case Management System so information contained therein is secure. Should the system be subject to a Freedom of Information Act request, the same protections would apply as currently do to law enforcement sensitive information. The following is collected:

- Record of Inquiry-TECS (ROIT)[12] – This form is currently used to record the search criteria queried and the results of those queries;
- FBI Fingerprint Check – Provides summary information of an individual's administrative or criminal record within the United States and is conducted through the FBI's Next Generation Identification (NGI)[13] System. Query results provide all biographic data of individuals reported to the FBI that match the fingerprints in the Next Generation

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION (CBP), PRIVACY IMPACT ASSESSMENT FOR THE TECS, DHS/CBP/PIA-009, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SYSTEM (CPMS), DHS/USCIS/PIA-060, *available at*https://www.dhs.gov/uscis-pias-and-sorns.

[12] TECS is used to assist federal, state, and local law enforcement and intelligence agencies identifying individuals who pose a risk to National Security and/or public safety; Prevent ineligible aliens from obtaining immigration benefits; and Identify petitioners ineligible to file family-based immigrant visa petitions in accordance with the Adam Walsh Act.

[13] *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION IDENTIFICATION, *available at* https://www.fbi.gov/services/freedom-of-informationprivacy-act/department-of-justicefbi-privacy-impact-assessments#:~:text=Department%20of%20Justice%2FFBI%20Privacy%20Impact%20Assessments%20%28PIAs%29%20THE,APPLICABLE%20LEGAL%2C%20REGULATORY%2C%20AND%20POLICY%20REQUIREMENTS%20REGARDING%20PRIVACY.

Identification System. These results are maintained in CPMS. There are three definitive results queried in CPMS (IDENT,[14] Non-IDENT, and Unclassifiable) to retrieve the Identity History Summary (IdHS - formerly known as Record of Arrest (RAP) sheet). The data collected is identified below:

- Names or aliases;
- FBI Name Check or FBI information and/or number;
- Fingerprint Identification Number (FIN);
- Addresses;
- Date of birth;
- Country of birth;
- Height and weight;
- Gender;
- Personally identifiable information related to the nature of fraud suspicion, and associated details;
- Personally identifiable information related to the results of fraud investigations;
- Resolution Memoranda: record the disposition of TECS, and other system "hits;" and
- Discussions among AAO staff regarding any manner of Fraud Detection and National Security action that may be required in a case.

AAO personnel load information into the AAO Case Management System by attaching electronic files to records or via manual-entry into data fields. The AAO officers can add, delete, or modify the information stored in the AAO Case Management System as needed to during their normal course of business. Once the background clearance is completed, the final background clearance information is stored in the AAO Case Management System and becomes a permanent record in accordance with the retention schedule.

AAO personnel assigned to an appeal, motion, or certification review all case-related information provided by the individual, including supplementary evidence, and review the A-File or receipt file to determine the benefit eligibility of the individual.

[14] The "Non-IDENT" and "IDENT" fingerprint results are not acronyms. The "IDENT" fingerprint result should not be confused with the IDENT system, which is the biometric repository system managed by the DHS Office of Biometric Identity Management (OBIM).

# Privacy Impact Analysis

### Authorities and Other Requirements

The legal authority to collect this information in AAO Case Management System does not change with this update. The legal authority to collect information and associated evidence on each benefit application[15] is under 8 CFR §§ 103.3 and 103.5. The AAO uses the information the applicant/petitioner provides on the Form I-290B to adjudicate appeals or motions on decisions under immigration laws.

The collection, use, maintenance, and dissemination of information are covered under the following system of records notices (SORN):

- Alien File, Index, and National File Tracking,[16] which covers the collection, use, maintenance of appeals, motions, certifications, and supplemental evidence;
- Benefit Information Systems,[17] which covers the collection and use of appeal and motion applications, decisional data, and associated fees; and
- Immigration Biometric and Background Check (IBBC) System of Records,[18] which covers the collection and use of biometric and background check results.

This update does not change the Authority to Operate (ATO) for AAO Case Management System. The AAO Case Management System is covered as a minor application under the Salesforce Hosting Environment. USCIS completed the Salesforce Hosting Environment security assessment and authorization documentation on December 17, 2018, and was subsequently enrolled in the USCIS Ongoing Authorization Program.

The National Archives and Records Administration (NARA) approved the AAO Case Management System retention schedule DAA-0566-2016-0001 on June 5, 2016. This retention schedule states that all records on an individual with an associated case(s) should be destroyed 25 years from the individual's latest case completion date. Records on an individual without an associated case should be destroyed 25 years from record creation date. Records that are linked to

[15] The AAO's appellate authority was afforded by the Secretary of DHS in 2003. The Delegation Memorandum (0150.1, 3/1/2003) references 8 CFR 103.1(f)(3)(E)(iii), which is no longer in effect (but does lend itself to understanding the AAO's authority). The Delegation Memorandum gives AAO appellate authority, not the Immigration and Nationality Act or anything specific in Title 8 of the Code of Federal Regulations. Authority to collect is as stated both here in this Privacy Impact Assessment and the Privacy Act Statement on the I-290B form instructions.
[16] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.
[17] *See* DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] *See* DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

national security, law enforcement, fraud, administrative investigations or actions, congressional inquiries or similar matters may be extended beyond the applicable 25-year period in five-year increments.

The AAO Case Management System maintains information from the Form I-290B, *Notice of Appeal or Motion*, that is subject to Paperwork Reduction Act (PRA) requirements. Form I-290B is subject to OMB Control Number 1615-0095.

**Characterization of the Information**

All appeals, motions, and certifications received by the AAO will be tracked in this system from arrival, through every touch point in the adjudication process so that every case can be tracked from start to finish. In this way, the "pending" cases will be known, as well as all cases assigned, on hold, and completed. Having a centralized tracking mechanism will reduce duplication of tracking efforts by 50% – 75%, as the three categories of cases (i.e., appeals, motions, certifications) have their own independent method to complete the adjudication process.

The AAO Case Management System collects the following data elements from other source systems or from forms directly collected from an applicant/petitioner:

- Appeal, motion, or certification;
- Date received by USCIS;
- Date received by AAO;
- Originating office;
- Assigned officer;
- Reopen date (in case of AAO Reopen on Service Motion);
- Appeal file number;
- Underlying petition receipt number;
- A-Number (when applicable);
- Name;
- Country of birth;
- Citizenship;
- Country of origin;
- Form type;
- Form appealed;

- Business name (where applicable);
- Attorney;
- Preparer of the form;
- Address;
- Associated cases (other closely related appeals);
- File location;
- Point in process (e.g., Mail room/in-processing, triage, pending, in adjudication);
- Decision (e.g., approved, rejected, withdrawn);
- Date adjudicated;
- Status code;
- Case history (searchable);
- Comments (searchable);
- Correspondence tracking (searchable);
- Law enforcement sensitive information (e.g., TECS record number, record of inquiry - TECS (ROIT), hit resolution memo);
- Sensitive but unclassified information;
- Potential derogatory information;
- Written correspondence; and
- Written decision.

The AAO Case Management System creates reports on the timeliness of various steps in the adjudication process. In addition, it creates workload reports to measure the number of receipts, completions, and pending cases. The reports will help AAO leadership manage the office effectively and report on timeliness.

An extract of CLAIMS 3 or ELIS is uploaded into the AAO Case Management System to ensure accuracy of information contained in the system. Generally, information ingested into the AAO from CLAIMS 3 or ELIS will not change (in CLAIMS 3 or ELIS) while under review by the AAO.

The AAO Case Management System collects information submitted by the applicant/petitioner on the Form I-290B and by the attorney or representative on the Form G-28 (Notice of Entry of Appearance as Attorney or Accredited Representative), from CLAIMS 3 or

ELIS and from RAILS.[19] The AAO collects information from CLAIMS 3 and ELIS to reduce the amounts of manual data entry and potential errors. The AAO collects information from RAILS to determine the responsible party for the physical file.

The AAO Case Management System that the AAO facilitates imports CLAIMS 3, ELIS and RAILS data through Person Centric Query System.[20] The information coming from CLAIMS 3, ELIS and RAILS includes the receipt number/A-Number, originating office, and date received at USCIS. The additional data elements to include law enforcement sensitive, sensitive but unclassified, and potential derogatory information that Appeals Officers learn from TECS, Arrival and Departure Information System (ADIS),[21] Consular Consolidated Database (CCD),[22] FDNS – Data System (FDNS-DS),[23] Student and Exchange Visitor Information System (SEVIS),[24] and Automated Biometric Identification System (IDENT).[25] Law enforcement information obtained from these systems will be captured in the AAO Case Management System. USCIS AAO personnel manually enter the following data elements in CLAIMS 3 or ELIS:

- Date of birth of the individual filing the Appeal or Motion;
- An alternate or safe mailing address for Violence Against Women Act (VAWA), T,[26] U,[27] and Special Immigrant Juvenile cases; and

---

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR RAILS, DHS/USCIS/PIA-075, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SYSTEM (PCQS), DHS/USCIS/PIA-010, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION (CBP), PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM, DHS/CBP/PIA-024, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[22] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE, *available at* https://www.state.gov/privacy-impact-assessments-privacy-office/.

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR PROGRAM (SEVP), DHS/ICE/PIA-001, *available at* https://www.dhs.gov/privacy-documents-ice.

[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT, BENEFIT REQUEST INTAKE PROCESS, DHS/USCIS/PIA-061, *available at*, https://www.dhs.gov/uscis-pias-and-sorns.

[25] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM), PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATIC BIOMETRIC IDENTIFICATION SYSTEM, DHS/OBIM/PIA-001, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[26] Victims of Human Trafficking – T nonimmigrant status is a temporary immigration benefit that enables certain victims of a severe form of human trafficking (sex or labor trafficking) to remain the United States for up to four years.

[27] Victims of Criminal Activity – U nonimmigrant status is set aside for victims' crimes who have suffered mental or physical abuse.

- Results of background Check and Security Information (e.g., TECS record number, Record of Inquiry-TECS (ROIT), hit resolution memo, fingerprint check results, Validation Instrument for Business Enterprises (VIBE) results).[28]

USCIS relies on individuals and their accredited representative to provide accurate information. The aforementioned individuals are required to sign a statement certifying, under penalty of perjury, that the information included in the appeal and motion form and any submitted documents are complete, true, and correct.

Incoming Form I-290Bs are reviewed by USCIS staff at either a Service Center or Lockbox facility. AAO staff also checks the accuracy of the data entered into CLAIMS 3 or ELIS at various points throughout the process. USCIS has detailed Standard Operating Procedures for handling information collected for Form I-290B. These procedures ensure that all data fields are completed and describe how data entry personnel handle inconsistencies during data entry.

**Privacy Risk:** There is a risk that USCIS may inadvertently disclose special protected class data (VAWA, T, U, and Special Immigrant Juvenile Cases) without a need-to-know.

**Mitigation:** This risk is mitigated. The AAO Case Management System includes a warning banner to indicate that an individual is protected by 8 U.S.C. § 1367. Information tagged in CLAIMS 3 or ELIS as special protected class data, is also tagged, and associated with a banner in the AAO Case Management System. The warning banner helps users comply with 8 U.S.C § 1367(a), which prohibits DHS from making unauthorized disclosures of information related to certain protected classes of aliens, including applicants and recipients of T (victims of human trafficking) and U (victims of criminal activity) visas, and relief under the Violence Against Women Act of 1994 (VAWA). The warning banner makes AAO Case Management System users immediately aware that they are displaying a record relating to a protected individual and that specific procedure regarding the disclosure and use apply. Any record in the AAO Case Management System that displays this banner must be handled as Section 1367 Information in accordance with USCIS policy.

**Privacy Risk:** There is a risk that unnecessary data elements are copied from CLAIMS 3 or ELIS resulting in more data than required for operational needs being stored in the AAO Case Management System.

**Mitigation:** This privacy risk is partially mitigated because data copied from CLAIMS 3 and ELIS are limited to basic biographic data necessary to track appeals and individuals. CLAIMS 3 and ELIS will continue to serve as the official system of records for dates and actions on appeals, motions, and certifications. Although the official events are recorded in CLAIMS 3 and ELIS, the

[28] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE VALIDATION INSTRUMENT FOR BUSINESS ENTERPRISES (VIBE), DHS/USCIS/PIA-044, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

system does not support the workflow and case management functionalities the AAO needs to effectively manage its workload, which is the reason for developing the AAO Case Management System. USCIS developed the AAO Case Management System to track receipts efficiently and effectively, assignments of work to officers, adjudications, and administrative actions. CLAIMS 3 and ELIS remain the systems in which the official actions are recorded and viewed across USCIS.

**Privacy Risk:** There is privacy risk of overcollection because individuals must resubmit benefit request information to USCIS to initiate an appeal that was already submitted as part of their original application.

**Mitigation:** This risk is partially mitigated. To appeal a denied benefit, individuals must submit minimal biographic information required by the Form I-290B. Without that information, AAO adjudicators would not know that a benefit denial was appealed, nor would they know for which denied benefit (and on what grounds) that appeal was made. AAO adjudicators avail themselves of the entire Record of Proceedings. While it is always a risk that an adjudicator may request information that is not necessary to the proper adjudication of an appeal; such actions would fall within the realm of misconduct by the USCIS officer and result in adverse consequences for that officer.

**Uses of the Information**

The AAO plans to use the AAO Case Management System to store and communicate to adjudicators the results of background checks. Adjudicators will, instead of sifting through paper files (some of which will no longer be available), examine the results of background checks and weigh the impacts on fraud and national security matters. The AAO continues to use information stored and maintained in the AAO Case Management System to support and manage the administration and adjudication of all appeals, motions, and certifications under AAO jurisdiction. Although basic information on appeals, motions, and certifications is available from existing systems, the placement of this information in the AAO Case Management System will also assist AAO leadership in managing and reporting on the office's caseload.

**Privacy Risk:** There is a risk that authorized users could use the data for purposes inconsistent with the original collection or inconsistent with their authority.

**Mitigation:** The risk is mitigated. All records, including background checks, are protected from unauthorized access and use through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. USCIS limits access to personally identifiable information by employing role-based access controls. All USCIS employees and contractors are trained regarding the use of the database and the sensitivity of the information and are required to take annual security and privacy awareness training to ensure the safeguarding of materials contained in the background checks.

### Notice

The publication of this Privacy Impact Assessment update provides additional notice to the public. Also, each benefit request form, contains a Privacy Notice that provides notice to individuals about the collection, USCIS's 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. Individuals also receive notice through the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking, DHS/USCIS-007 Benefits Information System, and the DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) system of records notices.

### Data Retention by the Project

Since the publication of the original Privacy Impact Assessment, the National Archives and Records Administration approved the retention schedule DAA-0566-2016-001 for the AAO Case Management System on June 5, 2016. This retention schedule states that all records on an individual with an associated case should be destroyed 25 years from the individual's latest case completion date. Records on an individual without an associated case should be destroyed 25 years from record creation date. Records that are linked to national security, law enforcement, fraud, administrative investigations or actions, congressional inquiries or similar matters may be extended beyond the applicable 25-year period in five-year increments. There are no privacy risks to the retention of information under this approved National Archives and Records Administration retention schedule.

### Information Sharing

This update does not impact information sharing with internal or external entities. AAO does not engage in any regular information sharing initiatives within or outside of DHS. There is no privacy risk related to external information sharing because AAO does not share information outside of DHS.

### Redress

This update does not impact how access, redress, and correction may be sought through USCIS. USCIS continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with the Freedom of Information Act unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. U.S. citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a Privacy Act or Freedom of Information Act request to view his or her USCIS record, the request can be mailed to the following address:

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

Persons not covered by the Privacy Act or Judicial Redress Act are not able to amend their records through the Freedom of Information Act. Should a non-U.S. citizen find inaccurate information in his or her received through the Freedom of Information Act, he or she may visit a local USCIS Field Office to identify, provide evidence, and amend inaccurate records. There are no risks associated with redress, since USCIS affords individuals with opportunities for access and correction.

**Auditing and Accountability**

USCIS ensures that practices stated in this Privacy Impact Assessment update comply with federal, DHS, and USCIS policies, including USCIS privacy policies, Standard Operating Procedures, orientation and training requirements, rules of behavior, and auditing and accountability procedures. Additionally, USCIS employees and contractors are required to complete annual privacy and security awareness training to ensure their understanding of appropriate practices for properly handling and securing personally identifiable information.

USCIS continues to limit access to the AAO Case Management System to authorized USCIS employees and contractors with a valid need-to-know. Access privileges are limited by establishing role-based user accounts to minimize access to information that the user does not need to perform essential job functions. Moreover, USCIS limits access privileges for users by ensuring they have authorized logon credentials (i.e., DHS-issued user ID and password) linked to their established role-based user account.

## Responsible Official

Angela Washington
USCIS Privacy Officer
U.S. Department of Homeland Security
Angela.Y.Washington@uscis.dhs.gov
(240) 721-3701

## Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security