



Privacy Impact Assessment

for the

Content Management Services

DHS Reference No. DHS/USCIS/PIA-079(a)

October 15, 2024



**Homeland
Security**



Abstract

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is expanding its use of the Content Management Services (CMS) to ingest and manage immigration-related content from other producers of Alien File content (hereafter A-File), which includes U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), the Department of Justice's Executive Office for Immigration Review (DOJ-EOIR) Electronic Court of Appeals System (ECAS), and the Department of State (DOS). Content Management Services will also interface with USCIS's Person Centric Identity Services (PCIS) via an Application Program Interface (API).¹ This model for managing content aligns with USCIS's vision to move away from transaction-based processes and toward a process focused on delivering person-centric content. USCIS is updating this Privacy Impact Assessment (PIA) to describe the additional immigration-related content that Content Management Services will manage, the new interconnection with Person Centric Identity Services² via an Application Program Interface, and the new data sources included in the Content Management Services' Content Repository.

Overview

The A-File³ contains official immigration records of individuals as they pass through or interact with U.S. immigration and inspection processes. A-Files may include documents related to law enforcement actions against or involving the individual. USCIS serves as the custodian of each A-File and its content. The content may come from various sources, including USCIS systems; other DHS components such as ICE or CBP; the Justice Department's Executive Office for Immigration Review proceedings—including proceedings before Immigration Judges and the Board of Immigration Appeals (BIA); and DOS. USCIS is expanding its use of electronic immigration records content to gain efficiencies for those business processes that rely on A-Files. CMS will begin ingesting information obtained by DHS components (ICE and CBP) and by

¹ Application Programming Interface (or API) is a mechanism for two or more systems or services to communicate with each other and transmit information and data. They also control access to hardware devices and software functions that an application may not necessarily have permission to use.

² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC IDENTITY SERVICES INITIATIVE, DHS/USCIS/PIA-087 (2022), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

³ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>. A digital A-File is an electronic file that stores information about an individual's immigration history. Not all A-File content is electronic or online, but RAILS allows USCIS to locate where relevant electronic A-File content is stored or housed.



external U.S. government agencies (the Justice Department's Executive Office for Immigration Review and DOS) to create a more comprehensive immigration record.

CMS is a cloud-based platform that USCIS uses to manage immigration-related content. Users access CMS immigration-related content through a user interface called STACKS⁴ (not an acronym) or through separate interconnected systems.⁵ A variety of USCIS, ICE, and CBP systems use CMS as a backend/support repository to enhance their effectiveness. CMS supports document management, imaging, records management, immigration benefit adjudication and enforcement action workflow, and document-centric collaboration. The CMS platform is an extendible and highly scalable solution that exposes a robust set of Application Program Interfaces to other enterprise applications to enable core content-related functions. The goal is to present backend services that front-end/public-facing applications (e.g., myUSCIS,⁶ Freedom of Information Act (FOIA) Immigration Records Systems (FIRST),⁷ Global,⁸ and Customer Profile Management System (CPMS)⁹) interact with when content services are required. External application developers work against standard content Application Program Interfaces published and available through an enterprise Application Program Interface Gateway. The model for managing this content aligns with USCIS' vision to move away from transaction-based processes and toward a process focused on delivering person-centric content.¹⁰

While storage and retrieval of content is CMS' most visible function, content services will also provide rules, behaviors, and policies that can be defined for content types within a given domain (e.g., case evidence or FOIA responses). Additionally, the underlying content platform will provide capabilities such as multi-format rendition (e.g., thumbnails or Portable Document

⁴ STACKS is a digital file viewing and content management system for official immigration records, part of the Content Management system directly supporting eProcessing.

⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR CONTENT MANAGEMENT SERVICES, DHS/USCIS/PIA-079 (2019 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR MYUSCIS, DHS/USCIS/PIA-064 (2016), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FOIA IMMIGRATION RECORDS SYSTEM, DHS/USCIS/PIA-077 (2019), 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 ASYLUM DIVISION, DHS/USCIS/PIA-027(d) (2018), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SYSTEM, DHS/USCIS/PIA-060 (2018 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC IDENTITY SERVICES INITIATIVE, DHS/USCIS/PIA-087 (2022), available at <https://www.dhs.gov/uscis-pias-and-sorns>. Person-centric refers to aggregating biometric data, biographic information, immigration status, and immigration history into a single identity profile.



Format (PDF) renditions), records retention policies, and disposition schedules. The CMS platform builds upon core managed business capabilities that are extendible and can be used by different business applications.

Reason for the PIA Update

USCIS is expanding its use of CMS to ingest and manage immigration-related content from other producers of A-File content, including ICE, CBP, the Justice Department's Executive Office for Immigration Review's electronic Court of Appeals System (ECAS), and DOS. Additionally, CMS will interface with Person Centric Identity Services via an Application Program Interface call to generate an A-Number and electronic file resulting from ICE and CBP encounters with an individual who does not have a physical A-File or an existing paper-based A-File. The electronic "A-File" is the electronic record of proceedings created to store information related to an individual's immigration history. Not all A-File content is electronic or available online, but RAILS¹¹ (not an acronym) allows USCIS to locate where relevant electronic A-File content is stored or maintained. USCIS is updating this Privacy Impact Assessment to describe the additional immigration-related content CMS will manage, the new interconnection with Person Centric Identity Services via an Application Program Interface, and the new data sources included in CMS' Content Repository.

Person Centric Identity Services is an agency-wide effort to use enhanced business processes and emerging technologies to improve biographic and biometric reliability, accuracy, and completeness across USCIS and other DHS immigration-related systems. In this effort, a person's data is defined as biographic information and biometric attributes that describe a unique identity. Person data is information related to the individual and not the immigration benefit. Person Centric Identity Services' scope includes ingesting personal data in ICE and CBP systems. Person Centric Identity Services is used by ICE and CBP personnel to assist in identifying an individual who may have previously filed an immigration benefit with DHS or was encountered or apprehended by ICE or CBP personnel. Person Centric Identity Services then associates existing immigration records with that individual. If there are no previous records, Person Centric Identity Services creates new records, which may include assigning A-Numbers to newly encountered identities and creating electronic A-Files. These newly created A-Files will be stored as digital person records within CMS. Person Centric Identity Services does not collect new data elements, or seek to use personal data in a new manner. It is designed to strengthen linkages of biometric and biographic information to the correct A-File. Person Centric Identity Services seeks also to consolidate existing data so that a comprehensive person-centric view of an individual's

¹¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR RAILS, DHS/USCIS/PIA-075 (2018), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



interactions with DHS is achieved. CMS is comprised of several core components internal to the system's operations:

- **Content Repository:** The content repository is the centralized repository of digital content. Digital content may be text (such as electronic documents), multimedia files (such as audio o
 - myUSCIS;
 - Scan on Demand (SODA);¹²
 - Customer Profile Management System; and
 - FOIA Immigration Records Systems (FIRST).

New data sources include:

- JP Morgan Chase (JPMC) Lockbox;¹³
- USCIS Electronic Immigration System (USCIS ELIS);¹⁴
- Global (not an acronym);¹⁵ directly ingested scanned content from Service Centers;
- Case Scanning Portal (CSP);¹⁶
- Iron Mountain (contractor), and other immigration benefit adjudication offices;
- ICE systems such as Enforcement Integrated Database (EID)
- Arrest Guide for Law Enforcement (EAGLE);¹⁷ and
- CBP systems such as e3 Portal;¹⁸
- Unified Secondary (USEC);¹⁹ and
- Unified Immigration Portal (UIP).²⁰

USCIS is exploring adding content from the ICE Office of the Principal Legal Advisor (OPLA) Case Management System (OCMS),²¹ also known as Principal Legal Advisor

¹² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT PROGRAM, DHS/USCIS/PIA-003 (2007 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR ENTERPRISE GATEWAY AND INTEGRATION SERVICES, DHS/USCIS/PIA-080 (2019 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR USCIS ELIS, DHS/USCIS/PIA-056 (2018 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>

¹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION



Network (PLAnet) and will update this Privacy Impact Assessment if that occurs. The Principal Legal Advisor Network does provide the Office of the Principal Legal Advisor access to record contents within CMS. However, the Office of the Principal Legal Advisor uses record contents from CMS in removal proceedings before the Justice Department's Executive Office for Immigration Review. In general, items that are considered USCIS records content and historically managed as paper (e.g., A-File, Receipt File, Temporary File (T-File)) will be managed in a standard electronic repository that is made available to authenticated systems through Application Program Interfaces. Until complete digitization is achieved, some content will be managed in separate physical files supporting the specific business process.

In addition to managing "active" content as part of an ongoing case adjudication, CMS provides archiving and records management functions. For example, CMS functionality determines when a record may move to a different storage location (archival) for longer-term preservation under established record retention requirements. All content (active or archived) determined to be a part of the agency record copy have disposition schedules to manage long-term retention and eventual destruction or accessioning to the National Archives and Records Administration (NARA).

- **Content Application Program Interfaces:** The Application Program Interface supports system-to-system interconnections. CMS allows applications to create multiple versions of single documents and maintains each of these versions as part of an overall record. This functionality is delivered through secure Application Program Interfaces, where authorization to these Application Program Interfaces are managed through USCIS approved security

SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ASYLUM DIVISION, DHS/USCIS/PIA-027 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁶ The Case Scanning Portal enables the scanning and storing Immigration benefit case files.

¹⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015 (2011 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-ice>.

¹⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCEMENT/IDENT, DHS/CBP/PIA-012 (2012 and subsequent updates), *available at* www.dhs.gov/privacy-documents-us-customs-and-border-protection.

¹⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CUSTOMS AND BORDER PROTECTION UNIFIED SECONDARY (USEC), DHS/CBP/PIA-067 (2021 and subsequent updates), *available at* www.dhs.gov/privacy-documents-us-customs-and-border-protection.

²⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR UNIFIED IMMIGRATION PORTAL, DHS/CBP/PIA-072 (2022 and subsequent updates), *available at* www.dhs.gov/privacy-documents-us-customs-and-border-protection.

²¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR OFFICE OF THE PRINCIPAL LEGAL ADVISOR CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-036 (2013), *available at* <https://www.dhs.gov/privacy-documents-ice>.



mechanisms (e.g., two-way Secure Socket Layer (SSL)).²² Content that is added and managed in CMS is managed in several repositories. These Application Program Interfaces are the cornerstone for integration initiatives internally with Person Centric Identity Services and externally with ICE and CBP systems.

- **WebUI Components:** WebUI components, named STACKS, allow users to create, edit, and remove case content through a user interface as needed to reflect which records are relevant to the benefit adjudication or enforcement action (these actions are noted in an audit log). This also allows users to add notes to documents in a case. External systems may connect directly to STACKS using a standard URL to access records directly. For example, the RAILS (not an acronym) system links directly to a particular individual's records within STACKS.
- **Content Ingestion:** Content ingestion facilitates system integration that supports content ingestion from external content providers (e.g., DOS, ICE, CBP). Additionally, it is used to ingest legacy content from decommissioned system(s) as part of a migration process (e.g., Enterprise Document Management System (EDMS)).²³ Another example of content ingestion into CMS is the storage of content provided by the Enterprise Print Manager System (EPMS). The Enterprise Print Manager System is used to generate correspondence, notices, and documents in support of adjudicative actions. Since this correspondence is considered a part of the electronic record, the Enterprise Print Manager System will send these electronic files to CMS, where they will be stored with other information about the specific case.
- **Cryptographic Object Storage Service:** The cryptographic object storage service provides USCIS the capability to store content objects securely in a highly available, highly durable manner while retaining the ability to delete any individual content object in a manner that renders it permanently unrecoverable. The solution leverages existing Amazon Web Services (AWS) infrastructure in conjunction with Federal Information Processing Standard (FIPS) validated encryption and signing Software Development Kits and a Key Management System to provide a standardized, secure component that can be used by clients of CMS.

In accordance with USCIS' mission, USCIS interacts with applicants, petitioners, beneficiaries, and requestors as well as representatives, interpreters, preparers, sponsors, and civil surgeons. USCIS has a history of associating paper and electronic case records to individuals using A-Files. The A-Files and A-Numbers provide a person-centric mechanism for organizing paper and electronic records. CBP and ICE also rely on and contribute to the immigration records

²² Secure Sockets Layer is a security protocol that provides privacy, authentication, and integrity to Internet communications. Secure Sockets Layer eventually evolved into Transport Layer Security.

²³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT PROGRAM (IDDMP), DHS/USCIS/PIA-003 (2007 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



contained in the A-File to perform their missions to enforce the nation's immigration laws at the border and within the United States. Though USCIS is the custodian of the A-File, both CBP and ICE create, contribute to, and use A-Files to support DHS' mission. To streamline the processes of consuming A-File content data, USCIS and CBP established a connection between CMS and CBP's Unified Immigration Portal.

The CBP Unified Immigration Portal provides agencies involved in the immigration process with a method to view and access certain information from each respective agency from a single portal in real-time (i.e., as the information is entered into the source systems). The Unified Immigration Portal aggregates disparate data sources, links related data elements, and visualizes those data elements in one location using dashboards. In addition to being a visualization tool, the Unified Immigration Portal serves as a records and information broker for collecting A-File content created by CBP and ICE for permanent storage in CMS, which ultimately reduces the reliance on CBP and ICE contributing paper printouts to the paper A-File. By ingesting A-File content/records sourced into the Unified Immigration Portal, USCIS is advancing a department guiding principle to create efficiencies across its components to support its mission.

As part of the apprehension and booking process, CBP officers and agents must complete various charging documents and immigration forms. They collect information from the subject, and then generate these documents and forms using e3 or Unified Secondary, respectively. These forms are generated by e3/Unified Secondary²⁴ and are electronically signed by the processing and supervisory officers or agents and the individual apprehended by CBP.

USCIS also ingests into CMS A-File record content created during removal proceedings before the Justice Department's Executive Office for Immigration Review. Currently, ICE and CBP upload paper versions of the documents into CMS or interfile such documents in a physical A-File, which USCIS then manages as a paper record or scans into CMS and manages as an electronic record. The electronic Court of Appeals System is part of the Justice Department's Executive Office for Immigration Review's overarching information technology modernization effort to phase out paper-based filing and case processing for court-related records submitted and retained in electronic format. The electronic Court of Appeals System is now fully implemented at all immigration courts and the Board of Immigration Appeals to support the entire life cycle of immigration cases.²⁵

The DOS also contributes record content to the A-File, principally in visa adjudications following approval of immigration petitions by USCIS. The DOS transmits visa adjudication

²⁴ The Unified Secondary system facilitates the documentation of information obtained during the secondary inspection process to make a decision. Depending on the case disposition, Unified Secondary will recommend certain charging documents.

²⁵ "The electronic Court of Appeals System is available at all immigration courts and the Board of Immigration Appeals. Use of the system is mandatory as of February 11, 2022." <https://www.justice.gov/eoir/ECAS>.



determinations to CMS through the Immigrant Visa Content Service (IVCS).²⁶ DOS systems are integrated only with the Immigrant Visa Content Service and does not directly interface with CMS. CMS ingests the digitized immigrant visa petition records and stores them as A-File content within CMS. USCIS and the DOS will continue to improve system-to-system connections to increase the amount of record content DOS sends to USCIS, to facilitate more efficient exchange of immigration content between USCIS and DOS, and to enable USCIS to share immigration record content for authorized purposes relevant to its visa adjudications with the DOS. To that end, the DOS and USCIS are currently discussing options to directly integrate the DOS content systems, such as Consolidated Consular Database (CCD),²⁷ Immigrant Visa Information System (IVIS),²⁸ and Pre-Immigrant Visa Overseas Technology (PIVOT)²⁹ with CMS or enable direct access for DOS personnel to the STACKS interface. Such integrations will be documented in interagency agreement(s) to include records management procedures and relevant privacy protections. When these solutions are identified, USCIS will also publish updates to this Privacy Impact Assessment accordingly.

Privacy Impact Analysis

Authorities and Other Requirements

The authority to collect information in CMS is set forth in the Immigration and Nationality Act, 8 U.S.C. §§ 1101, 1103, 1304, et seq., and in the implementing regulations found in volume 8 of the Code of Federal Regulations (CFR).

CMS serves as one of USCIS' repositories for the management of digital and electronic immigration-related records content. The Alien File, Index, and National File Tracking System of Records Notice³⁰ provides information about the collection, maintenance, use, and dissemination of digital immigration records and supporting documentation in CMS. As new sources are added, any relevant additional SORNs that describe those new sources will be included in updates to this Privacy Impact Assessment. The specific System of Records Notices covering the CBP and ICE³¹

²⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT PROGRAM, DHS/USCIS/PIA-003 (2007 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

²⁷ See DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR CONSULAR CONSOLIDATED DATABASE, *available at* <https://www.state.gov/privacy-impact-assessments-privacy-office/>.

²⁸ See DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR IMMIGRANT VISA INFORMATION SYSTEM, *available at* <https://www.state.gov/privacy-impact-assessments-privacy-office/>.

²⁹ See DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR PRE-IMMIGRANT VISA OVERSEAS TECHNOLOGY, *available at* <https://www.state.gov/privacy-impact-assessments-privacy-office/>.

³⁰ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed Reg. 43556 (September 18, 2017), *available at* <https://www.dhs.gov/system-records-notices-sorns>.

³¹ See DHS/USCIS/ICE/CBP-001 Import Information System, 81 Fed Reg. 48826 (July 26, 2016), *available at* <https://www.dhs.gov/system-records-notices-sorns>.



connected systems' collection, use, maintenance, and dissemination of information within CMS, as well as the relevant Justice Department's Executive Office for Immigration Review and DOS System of Records Notices from which CMS will ingest immigration-related A-File content is described in the original CMS Privacy Impact Assessment.³²

CMS is a major application with an Authority to Operate (ATO) and has been accepted into the DHS Ongoing Authorization program. As part of the Ongoing Authorization program, CMS' security and privacy posture is reviewed monthly using risk-based analysis tools to maintain its ATO.

CMS provides a digital repository service for immigration records relating to immigration benefit applications, petitions, and actions to enforce the nation's immigration laws. CMS does not have a records schedule but the records contained within CMS are subject to National Archives and Records Administration retention schedules on a form by form, benefit by benefit basis. The CMS architecture has the capability to apply specific retention schedule requirements to the records it contains to transfer records for archival storage or to the National Archives and Records Administration for permanent storage. This capability will be used once USCIS has completed its review and updates of the various specific retention schedules that govern content currently stored in CMS.

CMS is not subject to the Paperwork Reduction Act. CMS does not collect information directly from an individual; no forms associated with this collection. However, CMS stores electronic USCIS immigration request forms and FOIA/PA forms that the Paperwork Reduction Act covers. These immigration request forms are further discussed in DHS/USCIS/PIA-061 Benefit Request Intake Process,³³ while the DHS/USCIS/PIA-038 FOIA/PA Information Processing System discusses the FOIA/PA form.³⁴

Characterization of the Information

CMS serves as a repository of digital immigration-related record content. Digital content may be electronic documents, records, images, videos, or other binary files containing information. The digital content within CMS may include the following types of information:

- Immigration request forms;

³² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR CONTENT MANAGEMENT SYSTEM, DHS/USCIS/PIA-079 (2019), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

³³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT, FOR BENEFIT REQUEST INTAKE PROCESS, DHS/USCIS/PIA-061 (2016), *available at* <https://www.dhs.gov/privacy>.

³⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT, FOR FOIA IMMIGRATION RECORDS SYSTEM, DHS/USCIS/PIA-077 (2019), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



- Immigration-related law enforcement forms;
- Supplemental documents in support of an immigration request (e.g., birth certificates, passports, marriage certificates);
- Supplemental documents in support of an immigration law enforcement action (e.g., passports, identity documents);
- Biometric information provided as evidence in support of an immigration request or immigration law enforcement action (e.g., photographs, fingerprints, and signatures);
- Background check enforcement documents (e.g., Identity History Summary, previously known as the Rap Sheet);
- USCIS-issued notices and documents (e.g., Request for Evidence (RFE) and Notice of Intent to Deny (NOID));
- Notices to Appear, immigration judge orders, and other documents relating to removal proceedings;
- Audio and visual recordings (e.g., interviews);
- Responsive records to FOIA/PA requests; and
- Other documents (e.g., naturalization certificates, tax returns, labor certifications, correspondence, court dispositions, and interview notes).

These immigration documents may contain an array of information, including:

- First, middle, and last name;
- Alias(es);
- Sex;
- Address;
- Telephone number;
- Social Security number (SSN);
- A-Number;
- Passport Number;
- Date of birth;
- Country of birth;
- Country of citizenship;
- Vital documents (e.g., birth certificates, passports, marriage certificates);



- Biometric information provided as evidence in support of an immigration request or as part of an immigration law enforcement action (e.g., photographs, fingerprints, and signatures);
- Enforcement supporting documents; and
- Other documents (e.g., naturalization certificates; tax returns; labor certifications; correspondence; court dispositions; interview notes).

Information within CMS is originally derived from the following sources: (1) immigration requestors, beneficiaries, accredited representatives, attorneys, form preparers, interpreters, and/or other requestors; (2) internal DHS components; and (3) external entities. Most of the information in CMS is obtained from the data provided by the immigration requestor or beneficiary on the completed immigration request form and supporting documentation. CMS obtains data collected from individuals subject to immigration law enforcement actions or generated during removal proceedings through the connection with CBP's Unified Immigration Portal.

As part of the immigration record, CMS may maintain publicly available data from general internet searches and public social media content not protected by an individual's privacy settings. Pursuant to approved Social Media Operational Use Templates,³⁵ specially trained and authorized officers may conduct social media assessments³⁶ that USCIS adjudicators may consider verifying information provided by the requestor, investigate indications of fraudulent behavior, and identify threats to national security and public safety discovered while processing immigration benefit requests. This use of publicly available information is consistent with authority granted to USCIS by the Immigration and Nationality Act. This information is handled in a manner consistent with existing USCIS policies and rules of behavior regarding the use of social media information and publicly available information in adjudicative decision-making.

CMS depends on the accuracy and quality of information received from each source system or entity. All data is encrypted and is delivered "as is," except for reformatting to standardize the representation from the source system to CMS. This process ensures data integrity during transmission from the connected systems to CMS. Any data accuracy checks are accomplished at the connected system and are out of the scope of CMS and its security and privacy controls. CMS cannot and does not provide any assurance that the data it delivers is accurate.

³⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, DIRECTIVE NUMBER: 110-01 PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA (June 8, 2012), *available at* <https://www.dhs.gov/publication/privacy-policy-operational-use-social-media-directive-110-01>.

³⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DIRECTORATE, DHS/USCIS/PIA-013(a) (2019 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



Uses of the Information

CMS serves as a data repository for digital immigration content. The purpose of CMS is to collect, consolidate, and manage digital information that supports an individual's immigration history in a central location. CMS may receive immigration content through secured Application Program Interfaces from internal and external to DHS. CMS offers access to the digital immigration related content through two mechanisms: (1) by a user interface called STACKS; and (2) through an interconnected system.

CMS does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or anomaly.

DHS components (Headquarters, ICE, and CBP) will be able to access A-File record content maintained in CMS through the Unified Immigration Portal. ICE and CBP are creators, contributors to, and users of the A-File record content in CMS through the Unified Immigration Portal. Other DHS components may be given limited access as permitted by law or policy. Such access will be documented in Memoranda of Agreement/Memoranda of Understanding or other interagency agreements.

Notice

All persons are provided general notice of USCIS's use of CMS and CMS' connection with the Unified Immigration Portal through this Privacy Impact Assessment, source system Privacy Impact Assessments, and other component/agency Privacy Impact Assessments. The System of Records Notices applicable to the data visualized in the Unified Immigration Portal provide additional transparency. Moreover, when CBP collects information from persons entering the United States, CBP provides a form of notice through multiple signs posted in screening or processing areas at ports of entry. Individuals encountered between ports of entry may not be provided advance notice but will be provided general notice at the time the information is collected (e.g., during an inspection and apprehension). In addition, the forms DHS and other federal agencies use to collect information include, as appropriate, a Privacy Act Statement or Privacy Notice.

Data Retention by the Project

The official A-File record may take three possible forms: (1) Paper records contained within a physical A-File; (2) digital or electronic records contained in an electronic system like CMS or USCIS Electronic Immigration System; or (3) a combination of paper and electronic formats housed in both a physical A-File and electronic system(s). A-Files are permanent records maintained in accordance with the National Archives and Records Administration Records Retention Schedule N1-566-08-11. As such, DHS/USCIS transfers A-Files to the custody of the National Archives and Records Administration 100 years after the individual's date of birth.



Information Sharing

Requests to access immigration records in CMS records content and applications by USCIS, CBP, and ICE personnel are governed through myAccess, which is a centralized service used to request access to USCIS systems and accounts. myAccess is maintained by the USCIS Identity, Credential, and Access Management (ICAM) program,³⁷ and is the USCIS account role provisioning and management system that automates the approval process and provides authorization for user roles and the ability to gain access to USCIS IT systems. Access to immigration records in CMS by other DHS components through the Unified Immigration Portal is limited to those with a mission-related need-to-know. Access to CMS by other federal agencies such as DOS will be governed by separate Memoranda of Understanding or Memoranda of Agreement and associated Interagency Service Agreements. Records protected under 8 U.S.C. § 1367 and 8 CFR 208.6 will be marked, identified, and handled in accordance with the applicable confidentiality provisions before the disclosure of information. If there is a valid need to share the CMS data externally, it must be done in accordance with the A-File System of Records Notice and DHS policy.

Redress

Individuals may seek access to their USCIS records by filing a Privacy Act or FOIA request. Only U.S. citizens, Lawful Permanent Residents (LPR), and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or the Judicial Redress Act may still obtain access to records consistent with a FOIA request 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 a FOIA request to view their USCIS record, they may file the request electronically at <https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act> or 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 request because information may contain sensitive information law enforcement, the release of which could compromise ongoing criminal investigations. Further information about the Privacy Act and FOIA requests for USCIS records can be found at <https://www.uscis.gov>.

³⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PERSONAL IDENTITY VERIFICATION (PIV) MANAGEMENT SYSTEM, DHS/ALL/PIA-014 (2006 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-department-wide-programs>.



Auditing and Accountability

In accordance with DHS security guidelines, CMS has auditing capabilities that log user activities. CMS tracks all user actions via domain security audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. CMS employs auditing measures and technical safeguards to prevent the misuse of data. In addition to general users of A-File record content, some CMS users have job duties that require them to design, develop, and optimize the system. These users perform this work under supervisory oversight. In addition, CMS has internal audits separate from the domain security audits; therefore, a double layer of audit trails exists. Furthermore, CMS is housed in the Federal Risk and Authorization Management Program (FedRAMP)-approved Amazon Web Services cloud environment, at a moderate confidentiality that allows USCIS to host personally identifiable information. Amazon Web Services US East/West is a multi-tenant public cloud designed to meet a wide range of regulatory requirements, including Government compliance and security requirements. FedRAMP is a U.S. Government wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

Responsible Official

Angela Washington
USCIS Chief Privacy Officer
U.S. Department of Homeland Security
Angela.Y.Washington@uscis.dhs.gov
(202) 570-8327

Approval Signature

Original, signed copy on file at the DHS Privacy Office

Deborah Fleischaker
Chief Privacy Officer (A)
U.S. Department of Homeland Security
privacy@hq.dhs.gov



APPENDIX D: DHS and External System Interconnections

*This Appendix mirrors Appendix D in the original CMS Privacy Impact Assessment

Below are the DHS and External System Interconnections with CMS

Connection Relationship	System	Information	Connection Type	Connection Subtype
CMS Receives from	Central Index System 2 (CIS2)	Person biodata and sensitivity status Violence Against Women Act (VAWA), Section 1367)	Direct Connection	Application Program Interface (API) - Gateway
CMS Sends to	CIS2	Person metadata (Alien Number)	Direct Connection	API - Gateway
CMS Receives From	Computer Linked Application Management System (CLAIMS) 3 LAN	Case Decision Metadata	Direct Connection	API - Gateway
CMS Sends to	CLAIMS 3 LAN	API Confirmation / Error Responses; Case and Content Metadata	Direct Connection	API - Gateway
CMS Receives From	Customer Profile Management System (CPMS)	Migration of CPMS Data to CMS Repository; Content and Metadata	Direct Connection	API - Gateway
CMS Sends To	CPMS	API Confirmation / Error Responses; Content and Metadata	Direct Connection	API - Gateway
CMS Receives From	Case Scanning Portal (CSP)	Scanned/digitized cases and content	Direct Connection	Kafka - Enterprise Messaging (USCIS only)
CMS Sends To	CSP	Confirmation/error responses	Direct Connection	Kafka - Enterprise Messaging (USCIS only)
CMS Receives From	Data and Business Intelligence Services (DBIS)	Case decision data related to closed cases received from Iron Mountain	Direct Connection	API - Gateway
CMS Sends To	DBIS	Case metadata	Direct Connection	API - Gateway



CMS Receives From	Enterprise Document Management System (EDMS)	Migration of EDMS A-File and Case content and metadata to CMS Repository	Direct Connection	API - Gateway
CMS Sends To	EDMS	API Confirmation / Error Responses	Direct Connection	API - Gateway
CMS Receives From	Electronic Print Management System (EPMS)	Correspondence related to Benefit Application Cases	Direct Connection	API - Gateway; Kafka - Enterprise Messaging (USCIS only)
CMS Sends to	EPMS	Kafka and API Confirmation / Error Responses	Direct Connection	API - Gateway; Kafka - Enterprise Messaging (USCIS only)
CMS Receives From	Fraud Detection & National Security Next Generation (FDNS NexGen)	Content and Metadata	Direct Connection	API - Gateway
CMS Sends To	FDNS NexGen	API Confirmation / Error Responses; Encounter Content and Metadata	Direct Connection	API - Gateway
CMS Receives From	Fraud Detection & National Security Data System (FDNS-DS)	Migration of FDNS Data to CMS Repository; Content and Metadata	Direct Connection	API - Gateway
CMS Sends to	FDNS-DS	API Confirmation / Error Responses	Direct Connection	API - Gateway
CMS Receives From	FOIA Immigration Records System (FIRST)	Content and Metadata	Direct Connection	API - Gateway
CMS Sends To	FIRST	Content and Metadata	Direct Connection	API - Gateway
CMS Receives From	Global Asylum	Case Decision Metadata	Direct Connection	API - Gateway; Kafka - Enterprise



				Messaging (USCIS only)
CMS Sends to	Global Asylum	API Confirmation / Error Responses; Case and Content Metadata	Direct Connection	API - Gateway; Kafka - Enterprise Messaging (USCIS only)
CMS Receives From	Iron Mountain	Scanned/digitized persons, cases and content	Indirect Connection	External FILE (Iron Mountain)
CMS Sends To	Iron Mountain	Confirmation/error responses	Indirect Connection	External FILE (Iron Mountain)
CMS Receives From	Immigrant Visa Content Service IVCS	Migration of IVCS data to CMS Repository	Direct Connection	API - Gateway
CMS Receives From	JP Morgan Chase (JPMC) Lockbox	Scanned/digitized cases and content	Indirect Connection	External Messaging (ActiveMQ)
CMS Sends To	JPMC	Confirmation/reconciliation/error responses	Indirect Connection	External Messaging (ActiveMQ)
CMS Receives From	MyUSCIS	I-539 Forms and Evidence, I-589 Forms and Evidence	Direct Connection	API - Gateway; Kafka - Enterprise Messaging (USCIS only)
CMS Sends to	MyUSCIS	Kafka Confirmation / Error Responses	Direct Connection	API - Gateway; Kafka - Enterprise Messaging (USCIS only)
CMS Receives From	Person Centric Query Service (PCQS)	Person Metadata	Direct Connection	API - Gateway
CMS Sends to	PCS	API Confirmation / Error Responses	Direct Connection	API - Gateway
CMS Sends to	RAILS	Notification of Digitized Cases and A-Files	Direct Connection	Kafka - Enterprise Messaging (USCIS only)



CMS Receives From	Scan on Demand Application (SODA)	Digitized A-Files	Direct Connection	Kafka - Enterprise Messaging (USCIS only)
CMS Receives From	CBP's Unified Immigration Portal (UIP)	A-File Create Messages, Alien Encounter Forms and Evidence	Direct Connection	API - Gateway
CMS Sends To	UIP	API Confirmation / Error Responses; Encounter Content and Metadata	Direct Connection	API - Gateway