Privacy Impact Assessment
for the

Content Management Services
(CMS)

DHS/USCIS/PIA-079

May 13, 2019

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

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

Abstract

U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), developed the Content Management Services (CMS), a cloud-based platform for use across USCIS to manage immigration-related electronic content and services. CMS serves as a backend repository of all digital immigration-related content to be accessed and retrieved through a user interface called STACKS (not an acronym), or through separate USCIS interconnected systems. USCIS is conducting this Privacy Impact Assessment (PIA) to analyze the privacy impacts associated with CMS, including STACKS, because this system collects, uses, stores, and disseminates personally identifiable information (PII).

Overview

In carrying out and overseeing the mission of lawful immigration to the United States, USCIS and its predecessors collected a significant amount of information from individuals and relied heavily on a paper-based process. Before the creation of Alien Files (A-Files),[1] many individuals had more than one file with the agency, oftentimes requiring personnel to initiate a labor-intensive process to search multiple systems and indexes. In an effort to eliminate this process and efficiently organize and index its records, the legacy Immigration and Naturalization Service (INS) issued each non-citizen a unique Alien Number (A-Number) and created individual files, called A-Files. Existing immigration files were also consolidated into A-Files for every individual. By introducing A-Files and issuing each individual an A-Number, INS created one file containing all immigration-related records for each individual.

USCIS presently receives approximately six million immigration requests[2] each year, which are comprised of many types of applications and petitions. Until recently, USCIS has used a paper process to verify the identities of immigration requestors,[3] adjudicate immigration requests, and share information with other government agencies to identify individuals who may pose a threat to national security and/or public safety. USCIS has also used separate electronic systems to accept electronically filed immigration request forms, manage workflows, and track the many paper and electronic records about an individual. Even with these electronic systems, most of the adjudicative process was reliant upon the use and maintenance of paper files. The electronic systems were also confined to specific benefit types or operational offices, which limited the ability

[1] The A-File contains official immigration records of persons who are not citizens or nationals of the United States, including records created as the individual passes through the U.S. immigration and inspection processes and, when applicable, records related to any law enforcement action against or involving the alien. See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[2] For purposes of this document, the term "immigration request" includes all benefit requests (as that term is defined in 8 CFR § 1.2) as well as other immigration-related requests handled by USCIS that are not considered benefits (e.g., deferred action).
[3] The term "immigration requestor" means someone who has filed an immigration request.

to integrate USCIS operations overall.

Because these paper processes are less efficient than electronic processes, USCIS started to shift away from a paper-based environment by using electronic systems and digitizing existing paper A-Files to create electronic images of the files. The goal of digitizing A-Files was to create a comprehensive view of an individual's immigration history, as well as to make files readily available to multiple users at the same time without the risks and costs associated with shipping and handling paper records. However, digitizing existing paper records and incoming paper records still proved to be timely and costly for USCIS.

ePROCESSING INITIATIVE

USCIS is operating under an eProcessing initiative to improve operational efficiency and customer service, and to strengthen the security and integrity of the immigration system. Under this initiative, USCIS plans to exclusively receive immigration request forms electronically, request evidence electronically from applicants and petitioners (collectively referred to as immigration requestors) and legal representatives, and use those digital records in the adjudication process. As part of the eProcessing initiative, USCIS is moving from a paper-based environment to a digital environment in which filing, adjudication, and communication are all electronic. This initiative proactively creates digital records, and minimizes the intake, handling, and digitization of new paper benefit filings. As USCIS moves towards a digital environment, USCIS is fundamentally shifting its immigration records management policies, processes, and technologies. The ultimate goal is for USCIS to create digital immigration records at the point of receipt that serves as the official record throughout the immigration lifecycle.[4]

USCIS developed CMS to serve as a core technical enhancement of the eProcessing initiative for the storage and management of digital immigration-related content in support of intake, case adjudication, and records management. USCIS plans to index records using an unique identifier (i.e., Receipt Number and/or A-Number) that is linked with associated benefit filings in CMS to follow a person-centric model, meaning digital records are efficiently organized and managed pertaining to a particular individual who interacts with USCIS. A person-centric model goes beyond simply associating case records to an individual. This model provides a consolidated view of an individual's entire immigration history through the digital content associated with his or hers interactions. Using a person-centric approach, USCIS has a holistic and easily accessible set of records pertaining to that individual and his or her identity during the benefit adjudication or other decision-making processes.

CONTENT MANAGEMENT SERVICES

CMS is a platform that facilitates USCIS' management of electronic content and services.

[4] Immigration files currently in paper form will remain as such until an individual affirmatively requests an additional benefit or until the record is otherwise used in an administrative context.

Specifically, it serves as the backend repository for the management of digital immigration-related content in support of immigration benefits, consistent with the Immigration and Nationality Act (INA), and of record requests made under the Freedom of Information Act and Privacy Act (FOIA/PA). USCIS has historically relied on existing systems, such as the Enterprise Document Management System (EDMS),[5] Microfilm Digitization Application System (MiDAS),[6] and the content repository of USCIS Electronic Information System (USCIS ELIS),[7] to store and preserve core digitized USCIS records (e.g., A-File, Receipt File, Temporary File) and historical immigration records. CMS will eventually replace the backend content repository of EDMS, MiDAS, and USCIS ELIS, and USCIS will migrate existing and historical records into CMS to digitally preserve the official and historical value of records. These systems will remain operational and available for use until their respective records are fully migrated into CMS. USCIS also uses CMS to maintain other digital immigration-related information (e.g., Freedom of Information Act (FOIA) and Privacy Act amendment requests).

Type of Content

Digital content may take the form of electronic documents, records, images, videos, or other binary files containing information. The digital content within CMS may include the following information:

- Immigration Request Forms;
- Supplemental Documents in support of an Immigration Request (e.g., birth certificates, passports, marriage certificates);
- Biometric Information in support of an Immigration Request (e.g., photographs and signatures);
- 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));
- Audio and visual recordings (e.g., interviews);
- Responsive records to FOIA/PA requests;[8]
- Other Documents (e.g., naturalization certificates, tax returns, labor certifications,

[5] *See* DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP), *available at* https://www.dhs.gov/privacy.
[6] *See* DHS/USCIS/PIA-017(a) Microfilm Digitization Application System (MiDAS), *available at* https://www.dhs.gov/privacy.
[7] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* https://www.dhs.gov/privacy.
[8] Responsive records to FOIA/PA requests are kept in a separate repository from benefit request information.

correspondence, court dispositions, and interview notes);

CMS receives the above listed information from other USCIS systems. All USCIS systems exchange information through various data streaming services. The data streaming services are a combination of data delivery tools and connections to facilitate the seamless communication between different USCIS systems. CMS does not directly connect to any USCIS systems, but relies on the data streaming services to share information. USCIS uses data streaming services to integrate existing systems with new applications and support services. The integration with these data streaming services allows CMS to share and receive information from other systems without adversely impacting the availability of CMS.

In most circumstances, the digital immigration-related content (e.g., forms, Privacy Act responsive records, supplemental evidence) within CMS is derived from the subject of a record who is seeking an immigration benefit, service, naturalization, or in immigration enforcement proceedings with DHS, USCIS, or the legacy agencies. This information was and continues to be collected directly from the immigration requestor. In addition, DHS components (e.g., U.S. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)) and other external entities (e.g., Department of State) may contribute immigration content to CMS, as well as receive it. CMS also maintains records responsive to other non A-File information requests related to statistics, contracts, memoranda, etc. Please see Appendix A for a list of data sources.

Access to Digital Records in CMS

CMS is a dynamic and collaborative system that supports the management, creation, and modification of digital content through a user interface or through an interconnected system. CMS offers access to the digital immigration-related content through two mechanisms – (1) through a user interface called STACKS, and (2) through an interconnected system. Through both access mechanisms, CMS allows authorized users to create, edit, and remove content. When users perform actions within the interconnected systems, the outputs are sent from the interconnected systems to CMS to maintain in specific content repositories. The interconnected system is also able to retrieve the information from CMS and display the information to the user through its respective user interface.

STACKS

STACKS is the user interface that allows USCIS employees to view content within CMS. USCIS employees can use STACKS to view the immigration request form, evidence, and other case content that are received via myUSCIS and stored in CMS and used as part of the adjudication process.[9]

[9] USCIS allows certain immigration request forms and service types to be electronically completed and filed by

STACKS is accessible through:

1. **Direct User Interface:** Through the direct STACKS user interface, USCIS users are offered the following functionalities:
    - **Search** – Users have the ability to search for documents. Users search for documents based on specific searchable fields, including name, A-Number, Receipt number, date of birth, or a combination of these data elements.
    - **File Review and Upload** – Users have the ability to review case details, digital applications, and evidence submitted through myUSCIS, and upload additional USCIS content (e.g., Request for Evidence, Appointment Notices, and Notice for Intent to Deny).
    - **Document Notes –** Users have the ability to view notes, and add notes and tags associated with documents.
2. **Integrated STACKS Icon**: Through this access method, the STACKS icon is integrated within the respective case management system, enabling users to access the immigration content submitted by the immigration requestor (including a copy of the immigration request form in its entirety as well as all associated supporting evidence and documentation), and any other relevant immigration information stored in CMS. Only cases that were submitted via myUSCIS to USCIS will have this feature within the appropriate case management system. The relevant case management systems include CLAIMS 3,[10] GLOBAL (not an acronym),[11] Investor File Adjudication Case Tracker (INFACT),[12] USCIS ELIS.[13] When the user clicks the STACKS icon within the case management system, only relevant case-related information from CMS is displayed via the STACKS user interface. Through this access method, users are only able to retrieve and display immigration content; documents cannot be modified through the case management system. This access method provides easy access to relevant content without the USCIS user needing to separately access another system or file in support of the benefit adjudication process.

At this time, only USCIS employees have access to the information maintained in CMS

immigration requestors and/or legal representatives through myUSCIS Account Experience. For more information, s*ee* DHS/USCIS/PIA-071 myUSCIS Account Experience *available at* https://www.dhs.gov/privacy.

[10] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information System and Associated Systems (CLAIMS 3) *available at* https://www.dhs.gov/privacy.

[11] *See* DHS/USCIS/PIA-027(a) Asylum Division, *available at* https://www.dhs.gov/privacy.

[12] To be covered under the forthcoming Immigrant Investor Program PIA. INFACT is the system associated with the Immigrant Investor Program.

[13] *See* DHS/USCIS/PIA-056 USCIS Electronic Information System, *available at* https://www.dhs.gov/privacy.

via STACKS. USCIS may ultimately extend access to parts of CMS via STACKS to other DHS components, and to external entities consistent with their mission, legal authorities, purposes, and uses. USCIS will update this PIA when access is provided to other DHS and external users. Specific STACKS Connected Systems are noted in Appendix B to this PIA.

Interconnected Systems

In addition to the STACKS user interface, users and systems may also access and store other immigration-related content (e.g., FOIA and Privacy Act responsive records) in CMS through a separate system using the system's own user interfaces. For example, the FOIA Immigration Records System (FIRST) connects to CMS to retrieve immigration related content used to respond to FOIA and Privacy Act requests, as well as to store the redacted and non-redacted FOIA/PA responsive records.[14] The connected systems may retrieve and store information in CMS.

CMS tags and organizes incoming information depending on the type of content (e.g., immigration request forms, supplemental documents, responsive records to FOIA requests). The content type originally derives from the connected system. Depending on the content type provided by the connected system, CMS automatically tags and organizes the information into separate content repositories (i.e., responsive records to FOIA requests are separated from official records), which logically separates information into manageable buckets to prevent the intermingling of data and ensure the records are used for the purpose for which they were originally collected. In addition, via the STACKS user interface, USCIS users can tag content and update any erroneous tags. The connected systems are responsible for ensuring that only users with appropriate roles and permissions are granted access to specific records. Interconnected Systems are noted in Appendix C to this PIA.

Document Integrity and Security

CMS securely codes documents containing PII using unique private and public keys for each file that is encrypted and stored within CMS to prevent unauthorized access, modification, or use of data. The document is encrypted with the public key, and can only be decrypted with the private key. An encryption key is a security feature that converts data into an unreadable cipher in order to scramble and unscramble data. CMS uses a collection of complex algorithms to encrypt the original content. In order to reverse the encryption process, only the private key of that particular key pair can convert the information into a readable format.

Future Enhancements

USCIS is publishing this PIA to provide transparency to the overall use of CMS. This PIA

[14] *See* DHS/USCIS/PIA-077 FOIA Immigration Records System (FIRST), *available at* https://www.dhs.gov/privacy.

evaluates the PII collected, maintained, used, and disseminated in CMS and evaluates the privacy risks and mitigation strategies built into the system and its connections to other USCIS systems. USCIS plans to update this PIA as additional CMS functionalities are added to preserve the confidentiality, integrity, and availability of the information. USCIS also plans to update the appendices to this PIA as new sources and new users are added.

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 authority to collect information in CMS is set forth in the Freedom of Information Act of 1966, as amended (5 U.S.C. § 552), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), the Immigration and Nationality Act, 8 U.S.C. §§ 1103, 1103, 1304, et seq., and in the implementing regulations found in volume 8 of the Code of Federal Regulations (CFR).

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

CMS serves as the repository for the management of digital immigration-related content in support of USCIS' mission. The Alien File, Index, and National File Tracking SORN[15] covers the collection, maintenance, use, and dissemination of digital immigration records and supporting documentation in CMS. As new sources are added, SORN coverage for CMS will be extended to cover the content type ingested into and maintained by CMS. The specific SORNs covering the connected systems' collection, use, maintenance, and dissemination of information within CMS are described in the attached Appendices.

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

CMS is a major application that is currently undergoing the Authority to Operate (ATO) process. Upon completion of this PIA, CMS will be accepted into the Ongoing Authorization program. Ongoing Authorization requires CMS to be reviewed on a monthly basis and maintain its security and privacy posture to maintain its ATO.

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

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

USCIS is developing a retention schedule for CMS that is subject to final approval by NARA. The CMS retention requirements are determined by content type from the interconnected system. Until the retention period is approved by NARA, USCIS will retain all unscheduled records indefinitely. Once the period is established, USCIS will dispose the records once the retention period has been met.

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.

Not applicable. CMS is not subject to the Paperwork Reduction Act requirements. CMS does not collect information directly from an individual, and there are no forms associated with this collection. However, CMS stores digital USCIS immigration request forms and FOIA/PA forms that are covered by the Paperwork Reduction Act. These immigration request forms are further discussed in DHS/USCIS/PIA-061 Benefit Request Intake Process,[16] while the DHS/USCIS/PIA-038 FOIA/PIA Information Processing System discusses the FOIA/PA form.[17]

Section 2.0 Characterization of the Information

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

CMS serves as the repository of digital immigration-related content. Digital content may take the form of 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;
- Supplemental documents in support of an Immigration Request (e.g., birth certificates, passports, marriage certificates);
- Biometric information provided as evidence in support of an immigration request (e.g., photographs and signatures);
- Enforcement documents (e.g., Identity History Summary, previously known as the Rap Sheet);

[16] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* https://www.dhs.gov/privacy.
[17] *See* DHS/USCIS/PIA-038 FOIA/PA Information Processing System (FIPS), *available at* https://www.dhs.gov/privacy.

- USCIS-issued notices and documents (e.g., Request for Evidence (RFE) and Notice of Intent to Deny (NOID);
- 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);
- Alien 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 (e.g., photographs and signatures);
- Enforcement supporting documents; and
- Other documents (e.g., naturalization certificates; tax returns; labor certifications; correspondence; court dispositions; interview notes).

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

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 submitted supporting documentation accompanying his or her immigration request. Each data source will be further examined in an Appendix to this PIA.

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

As part of the immigration file, CMS may maintain publicly available data from general internet searches and public social media content that is not protected by an individual's privacy settings. USCIS uses this publicly available information to verify information provided by the requestor to investigate indications of fraudulent behavior and identify any threat to national security and/or public safety in the processing of his or her immigration request. This use of publicly available information is consistent with authority granted by the INA. 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.

2.4 Discuss how accuracy of the data is ensured.

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

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate information is transferred between CMS and the connected systems.

Mitigation: This risk is not mitigated. CMS places responsibility for the accuracy and quality of information on each connected system. CMS does not change data "in route" to the receiving system other than to provide standardized formatting of the data, such as date and time formatting.

Privacy Risk: There is a risk that the information maintained in CMS is inaccurate. As a result, USCIS will rely on inaccurate information, including social media findings, to make a benefit or request determination.

Mitigation: This risk is partially mitigated. USCIS relies on the totality of information received and reviewed to adjudicate a benefit. In many cases, information is collected directly from immigration requestor. USCIS presumes the information submitted is accurate and verifies the information against multiple sources during the review process. USCIS gives the immigration requestor multiple opportunities during and after the completion of the application process to correct information he or she has provided and to respond to information received from other sources, including social media. If the information could lead to a denial of the immigration request and if it is information of which the applicant is unaware, it would be provided to the immigration requestor in a Notice of Intent to Deny, in an interview, or in similar processes, and the immigration requestor would have an opportunity to review and respond.

Privacy Risk: There is a risk of multiple copies of the same records existing within CMS.

Mitigation: This risk is not mitigated. CMS does not take active measures to eliminate duplicate documents; however, it does make a fingerprint of each document received using a cryptographic hashing algorithm. This fingerprint of the document is stored as document metadata allowing duplicate files to be easily found through periodic scans.

Privacy Risk: There is a risk that information could be incorrectly associated with the wrong individual.

Mitigation: This risk is mitigated. USCIS indexes records in CMS using a unique personal identifier (e.g., A-Number or Receipt Number) to associate records to a particular benefit filing in the document repository. A unique personal identifier is used to distinguish an individual's records from all other records in the document repository. This ensures that records maintained in CMS are not inadvertently associated with the incorrect individual or benefit filing.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses 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 from both internal and external sources for consumption through secured APIs. CMS offers access to the digital immigration-related content through two mechanisms: (1) by a user interface called STACKS, and (2) though an interconnected system.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or

locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

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

No. Access to CMS through STACKS and interconnected systems is limited to USCIS employees at this time. USCIS plans to update this PIA as access to STACKS or through the interconnected systems are extended to other DHS components.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized use and access to the digital immigration content within CMS.

Mitigation: This risk is partially mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards, such as restricting access to authorized connected systems. CMS provides USCIS the capability to store digital immigration content securely. STACKS offers USCIS personnel access to CMS content directly or through a case management system (e.g., CLAIMS 3, GLOBAL, INFACT, and USCIS ELIS), or access to CMS content through a connected system with its own user interface (e.g., FIRST). Users seeking to directly access CMS via STACKS or through a connected system must request access through the existing and standard USCIS approval processes. Interconnected systems have the responsibility to control access of their own user population. CMS does not manage users gaining access through a system interconnection. The need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS and USCIS access controls and procedures.

Additionally, through the use of cryptography tools, CMS encrypts data at rest and in motion, as well as monitors data activity to verify and audit data that is stored in the cloud. Cryptographic techniques are used to authenticate documents, as well as the standard exchange of information. With cryptography, CMS transforms plain text, or other types of document formats (e.g., PDF), in a way that it becomes unusable to unauthorized recipients.

Privacy Risk: There is a risk that USCIS may inadvertently disclose special protected class data, such as data protected under 8 U.S.C. § 1367, outside of the permissible uses of the confidentiality provisions.

Mitigation: USCIS has partially mitigated this risk. STACKS and the connected systems display an alert message to indicate that an individual is protected by 8 U.S.C. § 1367. The feature complies 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). This ensures USCIS users are immediately notified that they are viewing a record relating to a protected individual and that specific procedure regarding the disclosure and use apply. Any record from CMS that displays this banner via the user interface must be handled as Section 1367 information in accordance with USCIS policy. USCIS is also exploring to determine whether requirements exist to protect other special protected class data in a similar manner.

DHS Privacy Office Recommendation*:* The DHS Privacy Office recommends USCIS develop a mechanism to transfer banner or caveat language between systems. This will ensure that recipients are aware of the protections surrounding Section 1367 information prior to use or any onward sharing.

Section 4.0 Notice

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

CMS does not collect information directly from individuals. Each USCIS connected system will provide notice through its PIA and associated SORN, which are available on the DHS Privacy Office website and/or published in the Federal Register.[18] USCIS is providing notice of CMS and STACKS' use of information through this PIA.

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

CMS does not collect information directly from the individual, which results in the inability for an individual to consent, decline, or opt out of his or her information being stored in CMS. However, in many cases, the information contained in CMS was originally collected directly from an immigration requestor. The submission of an immigration request is voluntary. Individuals who apply for USCIS benefits are presented with a Privacy Notice. In signing the immigration request, the immigration requestor authorizes USCIS to release the information contained within the form and supporting documentation, when necessary, for the administration and enforcement of the U.S. immigration laws. The Privacy Notice details the authority to collect the information requested.

All PII in CMS is extracted data from other systems as noted above. The notice procedures

[18] DHS PIAs and SORNs are available at https://www.dhs.gov/compliance.

are outlined in the connected system PIAs and associated SORNs.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not be aware that his or her information is stored in CMS and may be shared with other connected systems.

Mitigation: This risk is partially mitigated by publishing this PIA. USCIS also publishes separate PIAs for each connected system that will describe how CMS is used to share information with other systems. The collecting agency provides notice at the point of collection that the information may be shared with other federal, state, local, and foreign government agencies and authorized organizations in accordance with routine uses described in the associated published SORNs. External agencies may also provide notice through published Privacy Notices, PIAs, or SORNs.

Section 5.0 Data Retention by the project

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

USCIS is developing a retention schedule for CMS that is subject to final approval by NARA. The CMS retention requirements are determined by content type from the interconnected system.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: CMS does not have a NARA-approved records retention schedule, which could result in records being retained for longer than necessary.

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

Once a retention schedule is approved, USCIS plans to use Cryptographic Erasure to purge data in accordance with the appropriate retention schedule. Cryptographic Erasure erases the encryption key of the document. While the document remains within CMS, by erasing the original key, the data is effectively impossible to decrypt rendering the document unrecoverable.

Section 6.0 Information Sharing

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

USCIS is not granting external entities access to CMS at this time as part of normal agency operations. However, USCIS plans to replace the functionality of existing USCIS systems with CMS, which may eventually be accessible to external agencies through STACKS or connected systems. All future external access requests to CMS or any other USCIS system will be evaluated by USCIS. All access requests 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, 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. USCIS will update this PIA, as well as Appendix D, prior to granting access to external entities.In the event that digital immigration content is shared externally on an ad hoc basis, USCIS may share data from CMS consistent with the routine uses covered by the applicable SORN. USCIS reviews all ad hoc sharing requests to ensure the sharing is compatible with the request and will evaluate whether the records are protected by any special confidentiality provisions. Any special protected class record from CMS is to be marked, identified, and handled in accordance with the applicable confidentiality provisions, such as 8 U.S.C. § 1367, and USCIS policy prior to the disclosure information. If there is a valid need to share the CMS data externally, such as responding to an external federal agency's Request for Information for a law enforcement purpose, USCIS shares the data through a Computer Readable Extract (CRE). If USCIS approves an ad hoc CRE, USCIS and the receiving entity adhere to the DHS 4300A Sensitive System Handbook - Attachment S1 - Managing CREs containing Sensitive Personally Identifiable Information (PII).[19]

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

Before externally sharing information on an ad hoc basis, USCIS verifies that the sharing is for a purpose compatible with the original purpose for which USCIS collected the information through a process that involves USCIS Privacy, Office of Chief Counsel, Office of Policy and Strategy, and the program involved in the sharing. USCIS also verifies that the external sharing is consistent with the routine uses contained within the applicable SORNs. This may include for

[19] See DHS Sensitive Systems Policy Directive 4300A (2017).

purposes that facilitate immigration or ensure the overall integrity of the immigration process.

6.3 Does the project place limitations on re-dissemination?

At this time, USCIS does not share digital immigration content from CMS as part of normal agency operations. However, in some ad hoc instances, USCIS may share digital immigration content, and the requesting entity may incorporate the records from CMS into its own Privacy Act System of Records. The requesting entity is required to obtain authorization from USCIS prior to re-dissemination of USCIS information. Any limitation placed on re-dissemination is overseen by USCIS and memorialized by USCIS and the receiving entity.

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

USCIS maintains a record of disclosures via the USCIS CRE process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information shared as part of an external entities ad hoc request will be used beyond the purpose for which the information was originally collected.

Mitigation: This risk is mitigated. USCIS has a formal process in place to review and evaluate ad hoc information sharing requests. USCIS is careful to share data with external agencies that have a permissible legal authority and when the use is compatible with the purpose for which the information was originally collected. Prior to the disclosure of information, USCIS proper authorities review each ad hoc information request to ensure USCIS' adherence to federal, regulatory, statutory, Departmental and Component privacy requirements, mandates, directives, and policy. Each ad hoc request is independently evaluated to ensure the information requested is compatible with the purpose for which USCIS originally collected the information, there is a justified business need to share information with a requestor, and there are adequate privacy compliance documents are in place. USCIS also determines whether any special protected class protections and requirements apply to ensure the appropriate handling of data.

Section 7.0 Redress

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

An individual may seek access to his or her USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, Lawful Permanent Residents (LPRs), 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 JRA still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

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

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

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

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

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

USCIS notifies individuals of the procedures for correcting their information in this PIA, source system PIAs and SORNs, Privacy Notices, and through the USCIS website. Specifically, the SORNs listed in the Appendices provide individuals with guidance regarding the procedures for correcting information. Privacy Notices, including notice of an individual's right to correct information, are also contained on the instructions to immigration forms published by USCIS.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk associated with redress. USCIS provides individuals with access to their

records that are not subject to exemptions when requested through a FOIA or Privacy Act request. Individuals who are United States citizens or LPRs may submit a Privacy Act request to contest or amend information. Any person, regardless of immigration status, can come to a USCIS Field Office to update his or her records.

Section 8.0 Auditing and Accountability

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

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. Many users have legitimate job duties that require them to design, develop, and optimize the system. These users perform this work under supervisory oversight. USCIS requires each employee to undergo an annual security awareness training that addresses his or her duties and responsibilities to protect the integrity of the information. In addition, the CMS system has internal audits separate from the domain security audits; therefore, a double layer of audit trails exists.

Furthermore, CMS is housed in the FedRAMP-approved Amazon Web Services (AWS) cloud environment, at a moderate confidentiality that allows USCIS to host PII.[20] AWS US East/West is a multi-tenant public cloud designed to meet a wide range of regulatory requirements, including Government compliance and security requirements.[21] FedRAMP is a U.S. Government wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

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

All USCIS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements/Notices). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures. Leadership at each USCIS office is responsible for ensuring that all federal employees and

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

contractors receive the required annual Computer Security Awareness Training and Privacy training.

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

CMS offers USCIS personnel access to its content directly or through a case management system (e.g., CLAIMS 3, GLOBAL, INFACT, and USCIS ELIS) via the STACKS user interface, or via a connected system interface (e.g., FIRST). Users seeking to directly access CMS must request access through the existing and standard USCIS approval processes. Interconnected systems have the responsibility to control access of their own user population. CMS does not manage users gaining access through a system interconnection. The need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS and USCIS access controls and procedures.

The STACKS user interface and connected systems use role-based access controls and enforce a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is mapped to the set of system authorizations required to support the intended duties of the role (e.g., Asylum adjudicators have access to GLOBAL). The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with specific access rights.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

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

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

Privacy Risk: The data maintained by Amazon Web Services (AWS) for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the

CMS system, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[22]

Responsible Officials

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

Approval Signature

Original signed copy on file with the DHS Privacy Office.

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

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

APPENDIX A: CMS Data Sources

Below are the systems that transmit digital content to be stored in CMS.

myUSCIS is a public facing web application that allows USCIS customers to obtain accurate information related to the immigration process. myUSCIS leverages CMS to store documents for USCIS customers.

- **PIA:** myUSCIS Account Experience[23]
- **SORNs:**
  - Alien File, Index, and National File Tracking System of Records (A-File)[24]
  - Benefits Information System[25]
  - E-Authentication Records System of Records[26]

Enterprise Print Manager System (EPMS) is used to generate correspondence, notices, and documents in support of adjudicative actions. EPMS supports the generation and printing of notices and documents (i.e., Cards, Travel Documents, Correspondence) that is provided to the immigration requestor. Since this correspondence is considered a part of the electronic record, EPMS will send these electronic files to CMS, where they will be stored with other information pertaining to that case.

- **PIA:** Benefit Decision and Output Processes[27]
- **SORN:** Benefits Information System[28]

FOIA Immigration Records System (FIRST) is an online case management system that allows for submission of online FOIA requests and electronic delivery of responsive records. CMS serves as the data repository for all responsive records to FOIA requests.

- **PIA:** FOIA Immigration Records System (FIRST)[29]
- **SORNs:**

[23] *See* DHS/USCIS/PIA-071 myUSCIS Account Experience *available at* https://www.dhs.gov/privacy.
[24] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[25] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[26] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[27] DHS/USCIS/PIA-063 Benefit Decision and Output Processes, *available at* https://www.dhs.gov/privacy.
[28] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[29] *See* DHS/USCIS/PIA-077 FOIA Immigration Records System (FIRST), *available at* https://www.dhs.gov/privacy.

- DHS FOIA and Privacy Act Record System[30]
- E-Authentication Records System of Records[31]

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

APPENDIX B: STACKS Interconnections[32]

Below are the systems that enable access to digital content in CMS through STACKS.

Computer Linked Application Management System 3 (CLAIMS 3) provides USCIS with a decentralized, geographically dispersed Local Area Network-based mission support case management system. CLAIMS 3 leverages CMS to store case documents as they go through the eProcessing process.

- **PIA:** CLAIMS 3[33]
- **SORN:**
  - A-File[34]
  - Benefits Information System[35]

Investor File Adjudication Case Tracker (INFACT) provides the ability to link, track, and assign EB-5[36] filings as well as provide a holistic view of filings for an investor. It utilizes CMS to store documents.

- **PIA:** Forthcoming Immigrant Investor Program PIA
- **SORNs:**
  - A-File[37]
  - Benefits Information System[38]
  - Immigration Biometric and Background Check[39]

Global is a case management system that supports USCIS affirmative asylum, Section 203 of the

---

[32] USCIS uses data streaming services that act as intermediary messengers to effectively and efficiently share data between USCIS and external systems in near real-time. CMS will connect either directly to USCIS systems or through a messaging system to share data (e.g., Enterprise Gateway Integration Services (EGIS), Kafka, and the Enterprise Services Bus 2).
[33] *See* DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* https://www.dhs.gov/privacy.
[34] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[35] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[36] USCIS administers the Immigrant Investor Program. Under this program, entrepreneurs (and their spouses and unmarried children under 21) are eligible to apply for EB-5 benefits, including a green card (permanent residence) if they: (1) Make the necessary investment in a commercial enterprise in the United States; and (2) Plan to create or preserve 10 permanent full-time jobs for qualified U.S. workers. INFACT is the system associated with this program.
[37] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[38] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[39] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

Nicaraguan Adjustment and Central American Relief Act (NACARA § 203), credible fear, and reasonable fear cases. It provides the means for tracking of asylum cases as they progress from application filing through final determination/decision or referral to the U.S. Immigration Courts. CMS is leveraged to store files associated with case management.

- **PIA:** USCIS Asylum Division[40]
- **SORNs:**
  - A-File[41]
  - Asylum Information and Pre-Screening[42]
  - Immigration Biometric and Background Check[43]

[40] *See* DHS/USCIS/PIA-027(c) USCIS Asylum Division, *available at* https://www.dhs.gov/privacy.
[41] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[42] DHS/USCIS-010 Asylum Information and Pre-Screening, 80 FR 74781 (November 30, 2015).
[43] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

Appendix C: Connected Systems

Below are the systems that have direct access to the digital content within CMS.

FOIA Immigration Records System (FIRST) is an online case management system that allows for submission of online FOIA requests and electronic delivery of responsive records. FIRST uses CMS to store and retrieve documents for viewing within the system.

- **PIA:** FOIA Immigration Records System (FIRST)[44]
- **SORNs:**
  - DHS FOIA and Privacy Act Record System[45]
  - E-Authentication Records System of Records[46]

[44] *See* DHS/USCIS/PIA-077 FOIA Immigration Records System (FIRST), *available at* https://www.dhs.gov/privacy.
[45] DHS/ALL-001 DHS FOIA and Privacy Act Record System, 79 FR 6609 (February 4, 2014).
[46] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857, (August 11, 2014).

APPENDIX D: DHS and External System Interconnections

At the publication of this PIA, there are no internal or external DHS interconnected systems to CMS. USCIS will update Appendix D when new interconnected systems are added.