Privacy Impact Assessment

for the

USCIS Microfilm Digitization Application System

DHS Reference No. DHS/USCIS/PIA-017(b)

February 4, 2025

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), Immigration Records and Identity Services Directorate's (IRIS) Identity, Records, and National Security Delivery Division (IRSDD) manages the Identity and Information Management Division (IIMD) and operates the USCIS Microfilm Digitization Application System (MiDAS). MiDAS electronically stores historical immigration-related records and enables USCIS to search and provide records as appropriate to government agencies and members of the public who request this information. USCIS is updating this Privacy Impact Assessment (PIA) to permanently implement how USCIS currently uses MiDAS and to identify and mitigate privacy risks associated with the change and the use of personally identifiable information related to: (1) updating the names of the USCIS' division and branches responsible for operating MiDAS; and (2) the transfer of two subsystems, the Scan on Demand Application (SODA) system and the Document Services Management System (DSMS), from the Enterprise Document Management System (EDMS)[1] to MiDAS.

Overview

USCIS electronically maintains millions of immigration-related records that were created between 1893 and 1975 within MiDAS,[2] which serves as a static repository for these historical records and enables USCIS to search and provide these historical records as appropriate to government agencies and members of the public who request this information for mission-related and genealogy purposes. MiDAS preserves and digitally indexes over 85 million immigration-related records that were previously stored on microfilm. It contains historical records documenting the arrival and naturalization of immigrants who arrived in the United States between 1893 and 1975. Historic immigration-related records include index cards that reference over 20 different record series and immigration records. MiDAS converts index cards and records from deteriorating microfilm into digital images to improve retrieval of these historical records.

MiDAS is used to support USCIS Identity and Information Management Division, Records Division's Genealogy Services Branch (Genealogy) and the Office of Records Management (ORM). MiDAS provides government agencies and member of the public requestors the ability to perform search requests and file requests for historical immigration documents. USCIS employees from the Genealogy Services Branch and Office of Records Management can track the status of case requests, access immigration image files, and search for and analyze digitized indices. MiDAS

[1] USCIS officially dispositioned the Enterprise Document Management System on August 26, 2022.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE MICROFILM DIGITIZATION APPLICATION SYSTEM (MIDAS), DHS/USCIS/PIA-017 (2008 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

has a single repository for supporting all different types of files such as A-Files, Naturalization Certificate-Files (C-Files), Registration Forms, Visa Files, Registry Files, Master Index files, and Flex-o-Line files.

The Genealogy Services Branch and the Office of Records Management use MiDAS to respond to historical records requests made by government (federal, state, and local agencies) and member of the public requestors. Government agencies may use information obtained from MiDAS to assist the determination to grant or deny a government benefit or to conduct a law enforcement investigation. Members of the public may use information obtained from MiDAS to acquire historical immigration records for genealogical and other historical research. The Office of Records Management responds to requests from within DHS and its components (e.g., U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP)) and other government agencies[3] for historical records created between 1893 and 1975, and the Genealogy Services Branch responds to requests made by members of the public. The only genealogical records that can be requested by members of the public are for individuals who are deceased, and requestors must provide documented proof of death if the subject of the request was born less than 100 years before the date of the request. Anyone requesting records of a naturalization that occurred on or after April 1, 1956, or an arrival after May 1, 1951, must submit a Freedom of Information Act (FOIA) request.

MiDAS consists of the following components that allow for submission of a request and USCIS to search and retrieve matching records to respond to such a request.

External components used by requestors to request records:

- The Office of Records Management Web Request (ORM-WR)[4] site is used by federal, state, and local government agencies to request immigrant files and searches for immigrant files, file creations, Certificates of Non-Existence (CNE), and certified true copies.
    - Public users may make a Certificate of Non-Existence request by using the online request form located on the public Certificate of Non-Existence web page,[5] which is separate, but part of the Office of Records Management Web Request site. A Certificate of Non-Existence certifies that USCIS did not find the type of records identified by the requestor. If USCIS does finds the type of records specified by the

[3] These federal agencies mainly include the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Department of State (DoS), the Department of Defense (DoD), the Department of Justice (DOJ), the Department of Treasury, the Department of Transportation (DoT), the District of Columbia government, the Office of Personnel Management (OPM), the Social Security Administration (SSA), and the National Aeronautics and Space Administration (NASA).
[4] The Office of Records Management Web Request site is available at https://midas.uscis.dhs.gov/#/login.
[5] The Office of Records Management Web Request for Certificates of Non-Existence site is available at https://midas.uscis.dhs.gov/#/cne/request.

requestor, a Certificate will not be issued, but the requestor will be provided a response, such as the following:

"A record was located showing the subject is a naturalized citizen. Record Services only certifies the non-existence of record and no record of naturalization; therefore, your request does not meet the criteria for processing. You may choose to contact the Genealogy program at www.uscis.gov/genealogy or you can submit a FOIA request (Form G-639, available at www.uscis.gov under immigration forms)."[6]

- The Genealogy Web Request (GEN-WR)[7] site is used by the public to request immigrant files and searches for immigrant files.

Internal components used by USCIS Immigration Records and Identity Services (IRIS) Records Division (RD) to respond to requests:

- The MiDAS Search Engine (MSE) allows Immigration Records and Identity Services users to enter search criteria to locate and display specific records from a set of approximately 100 million digitized images created from deteriorating microfilm and paper files. The MiDAS Search Engine, used by both the Genealogy Services Branch and Office of Records Management, is a standalone search engine only accessible to appropriate users, and provides background research and information to agency leadership, public researchers, and preparers, promotes agency history, and provides timely public access to the agency's historical records.
- The Office of Records Management Case Management Tracking (CMT) subsystem is used as a case management tool (commonly known as customer relationship management system) to streamline the activities needed to complete a task and track and manage the fulfillment of requests, in the form of cases, for historical immigrant information from government agencies (e.g., provides the homepage, browser menu bar, application tool bar to print, query drop down list, create a new query, execute a chosen query, search for, and find records within the database).
- The Genealogy Services Branch Case Management Tracking subsystem is used as a case management tool to track and manage the fulfillment of requests, in the form of cases, for historical immigrant information from the public.

Historical Records

[6] Or directly at https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act
[7] The Genealogy Web Request is available at https://genealogy.uscis.dhs.gov/.

The Immigration Records and Identity Services, Records Division releases five types of agency historical records to requestors. The types of releasable historical records maintained by USCIS include:[8]

- **Naturalization Certificate-Files** (C-Files) are copies of records relating to naturalizations in federal, state, county, or municipal courts; overseas military naturalizations; replacement of old law naturalization certificates; and the issuance of Certificates of Citizenship in derivative, repatriation, and resumption cases. Naturalization Certificate-Files were created between September 27, 1906, and March 31, 1956. Naturalization Certificate-Files are a product of the Basic Naturalization Act of 1906, which created the Federal Naturalization Service and required the collection and maintenance of copies of all naturalization records nationwide. The Naturalization Certificate-Files series later expanded to include records of U.S. citizenship acquired by derivation (naturalization by virtue of a qualifying relationship to another who is a birthright or naturalized citizen) and resumption or repatriation by former U.S. citizens who expatriated themselves (i.e., lost their U.S. citizenship).
- **Registration Forms** (Forms AR-2 and AR-102)[9] are copies of approximately 5.5 million Registration Forms completed by all noncitizens aged 14 and older residing in or entering the United States between August 1, 1940, and March 31, 1944. The Alien Registration Program was a World War II-era national security measure ordered by the original Alien Registration Act of 1940. That 1940 Act directed the Immigration and Naturalization Service (INS) to fingerprint and register every noncitizen aged 14 and older living or arriving in the United States. Registration Forms document the presence of non-citizens in the United States during World War II. The legacy Immigration and Naturalization Service used the Form AR-2 to make a record of all noncitizens residing in or entering the country between August 1940, and March 31, 1944. Although stamped with an A-Number, AR-2s are a distinct records series and are not A-Files.
- **Visa Files** are original arrival records of immigrants admitted for permanent residence under provisions of the Immigration Act of 1924. Visa Files were created between July 1, 1924, and March 31, 1944. The Immigration Act of 1924 required all arriving non-citizens to present a visa when applying for admission to the United States. Immigrants requested visas at U.S. Embassies and Consulates abroad before

[8] *See* 8 CFR 103.39.
[9] Individuals submitted the Form AR-102 to satisfy the registration requirement between August 1, 1940, and March 31, 1944. *See* 8 CFR 170.8. (1938 & Supp. 1941).

their departure. The State Department only issued visa documents to approved immigrants and the Immigration and Naturalization Service only admitted immigrants arriving with a visa. In this way, visas allowed the federal government to both select and limit the number of immigrants lawfully admitted for permanent residence.

- **Registry Files** are records that document the creation of immigrant arrival records for persons who entered the United States prior to July 1, 1924, and for whom no arrival record could later be found. Registry Files were created between March 1929, and March 31, 1944. Registry Files document the creation of official immigrant arrival records under the Registry Act of 1929.[10] The Registry Act applied to persons who entered the United States prior to July 1, 1924, and for whom no arrival record could later be found. The Registry Program required applicants to document their arrival and subsequent residence in the country and Registry Files often contain significant biographical information about the subject.
- **A-Files** are the individual noncitizen case files that became the official file for all immigration and naturalization records created or consolidated since April 1, 1944. A-Numbers ranging up to approximately six million were issued to noncitizens and immigrants within or entering the United States between 1940 and 1945. The predecessor immigration agencies issued six to seven million series of A-Numbers between 1944 and May 1, 1951.

Reason for the Privacy Impact Assessment (PIA) Update

USCIS is updating the MiDAS Privacy Impact Assessment to document, analyze, and discuss the potential privacy risks associated with the system's use of personally identifiable information, specifically for system updates. These updates include changes to the names of the USCIS' division and branches responsible for operating MiDAS and documenting the transfer of two subsystems, the Scan on Demand Application system and the Document Services Management System to the MiDAS security authorization boundary.

Scan on Demand Application (SODA)

The USCIS National Records Center (NRC) uses the Scan on Demand Application to scan paper A-Files to create digital records. Most inactive paper A-Files are currently under the control of the USCIS National Records Center and the National Archives and Records Administration's (NARA) Kansas City Federal Record Center (KCFRC). The National Records Center is

[10] 45 Stat. 1512.

responsible for maintaining more than 25.1 million inactive A-Files and providing customers with timely access to information contained therein.

Since 2009, USCIS records digitized using the Scan on Demand Application were accessible via the Enterprise Document Management System. However, in 2022, USCIS officially dispositioned the Enterprise Document Management System as part of the agency's overall systems modernization efforts, and as of September 20, 2021, the Scan on Demand Application has transferred the digitized version of the paper A-Files to Content Management Services (CMS).[11] MiDAS itself does not store or ingest the Scan on Demand Application's data and the two systems do not share a direct connection.[12] After the conversion, the electronic file becomes an official A-File. This process enables the National Records Center to provide DHS personnel, who have been granted access via the Identity, Credential, and Access Management (ICAM) myAccess system[13] and who possess a need-to-know, with access to requested closed digitized A-Files.

The Scan on Demand Application enables Content Management Services to eliminate the need to mail the original physical paper A-Files to requestors, minimizing the potential for loss or the misplacement of A-Files, as well as saving the agency mailing costs. The Scan on Demand Application is also used to track requests received from ICE, CBP, and USCIS field offices that request A-Files be digitized and loaded into Content Management Services to serve an agency purpose. The need is typically triggered by submission of a benefit request, initiation of enforcement action, or receipt of a FOIA or Privacy Act (PA) request. After receipt of a request, USCIS personnel locate relevant A-Files, digitize the paper record using the Scan on Demand

---

[11] Content Management Services is a cloud-based platform for use across USCIS to manage immigration-related electronic content and services. Content Management Services serves as a backend repository of all digital immigration-related content to be accessed and retrieved through a user interface. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR CONTENT MANAGEMENT SERVICES (CMS), DHS/USCIS/PIA-079 (2019), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[12] The only relation the Scan on Demand Application has with MiDAS is that the Scan on Demand Application operates under MiDAS' Federal Information Security Modernization Act (FISMA) name, identification number, and security authorization. The Scan on Demand Application is also part of USCIS' Ongoing Authorization (OA) program. The Ongoing Authorization program reduces the time and effort for compliance testing, more efficiently allocates system-specific resources, ensures prompt identification of risks, and facilitates up-to-date knowledge and system documentation. It involves a shift from periodic to ongoing security assessments driven by risk. Ongoing Authorization tracks and reports security posture in near real time, leverages Continuous Diagnostics & Mitigation (CDM) technologies to support authorization and operational decisions, and monitors volatile controls through defined frequencies and documented testing processes as well as periodic and event-driven testing and assessments.

[13] The USCIS Office of Information Technology (OIT) complies with mandates pertaining to the Federal Identity, Credential, and Access Management (FICAM) program. USCIS Identity, Credential, and Access Management is an enterprise-wide program that collectively manages identity, credentials, access, and federation, and provides the integrity for internal USCIS, DHS component, and other government agency users for authentication and authorization for access to USCIS systems.

Application, and make the content and data available through a Content Management Services user interface called STACKS[14] (not an acronym). All digitized A-Files are stored in and available to authorized users through the Content Management Services system. The digitized paper files also contain A-File numbers, file locations, number of pages in the files, DHS employee names, the offices and agencies for which the employee works, and dates/times for actions taken to have files digitized as well as to have files removed from the Content Management Services system.

Only USCIS employees and contractors in the Scan on Demand Application team have access to its database where digitized paper files are held temporarily for quality assurance checks and in-transit to Content Management Services. Also, the database facilitates the digitization of requested files, tracking pending requests, and compilation of weekly, monthly, and yearly statistics related to the Scan on Demand Application. A portion of the database is used to track administrative and system errors. The system is set to collect all errors, alerts, and alarms; correlate them against the ruleset; and automatically escalate them, if needed, for resolution.

Document Service Management System (DSMS)

The USCIS Management Directorate, Office of Intake & Document Production (OIDP) operates the Document Service Management System, which is a web-based software solution used by offices to order blank USCIS internal and public facing paper forms (e.g., Form I-130, *Petition for Alien Relative*; Form N-400, *Application for Naturalization*; empty A-File jackets) and other documents such as information pamphlets, publications, and brochures. Like the Scan on Demand Application, the Document Service Management System's only relation to MiDAS is that it is now a subsystem within the MiDAS security authorization boundary, and has no direct connection. The Document Service Management System provides a centralized database for reports on the number of orders (e.g., statistical, or total numbers of a particular immigration benefit request form ordered by a specific directorate, program, or office within a specific period) from both the Office of Intake & Document Production's Eastern Forms Center (EFC) and Western Forms Center (WFC). The Document Service Management System provides tracking activities associated with version control and serialized items that reduce costs, and introduces greater efficiencies to the USCIS printing supply chain and forms management by identifying opportunities to standardize, consolidate, streamline, and eliminate obsolescence or duplication of the printed materials.

For example, the Western Forms Center utilizes the Document Service Management System to track, fulfill, and ship orders. Other offices use the Document Service Management System to order forms, track and review the status of orders, and receive orders from the Western Forms Center. The Document Service Management System also incorporates an online request

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

and approval process for secure forms. The system also improves efficiencies and reduces costs of printing and distributing USCIS documents. All forms and A-Files jacket requests ordered through the Document Service Management System are blank and sent to the requesting office without any personally identifiable information.

For USCIS employees and contractors to gain requestor access to the Document Service Management System they must first take the applicable required Document Service Management System training for one of the three types of Document Service Management System requestor modules listed below. USCIS employees and contractors requesting access must send the training certificate to the system's information technology program manager. In addition, if applicable, a memo signed by the Field Office Director (FOD) may be required to order secure documents or A-Files.

- Standard Requester Module – user is designated by their office to order standard (non-secure) documents;
- Secure Requester Module – user is designated by memo signed by Field Office Director to order secure documents or A-Files; and/or
- Approver/Endorser Module – user is designated by memo signed by Field Office Director to approve orders for secure documents or A-Files.

USCIS uses the requested attributes in a workflow to provision new users' accounts within myAccess. To maintain the security of these blank USCIS forms and documents, the designated requestor may not also be the designated approver for any given office. The Document Service Management System does not use passwords and login is granted via the Personal Identity Verification (PIV) card and the secure USCIS Identity, Credential, and Access Management/myAccess single-sign-on service (SSO). Once these have been reviewed by the Document Service Management System team, the user can request access.

Content Management Services (CMS)

Content Management Services is a platform that facilitates USCIS' management of electronic content and services and does not have a connection to MiDAS. 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, and of record requests made under FOIA and the Privacy Act. USCIS has historically relied on existing systems, such as the Enterprise Document Management System, MiDAS, and the content repository of USCIS

Electronic Information System (ELIS),[15] to store digitized USCIS records (e.g., A-Files, Receipt File, Temporary File) and historical immigration records. Content Management Services replaced the backend content repository of the Enterprise Document Management System. Content Management Services is also set to replace MIDAS and the USCIS Electronic Information System. USCIS will migrate both its existing and historical records into Content Management Services to digitally preserve the official records. These systems (MIDAS and USCIS Electronic Information System) will remain operational and available for use until their respective records are fully migrated into Content Management Services.

Types of Content

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

- Supplemental documents in support of an Immigration Request (e.g., birth and death certificates, passports, marriage certificates, naturalization certificates and certificates of citizenship);
- 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/Privacy Act requests;[16] and
- Other documents (e.g., tax returns, labor certifications, correspondence, court dispositions, and interview notes).

---

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

[16] Responsive records to FOIA/Privacy Act requests are kept in a separate repository from benefit request information.

The Content Management Services platform is a robust set of Application Programming Interfaces (API)[17] to enable functions. The goal is to present backend services that front-end/public-facing applications (e.g., myUSCIS,[18] Freedom of Information Act (FOIA) Immigration Records Systems (FIRST),[19] Global,[20] and Customer Profile Management System (CPMS))[21] interact with when content services are required. External application developers work with standard content Application Programming Interfaces that are published and available through an enterprise Application Programming Interfaces Gateway. The model for managing this content aligns with USCIS' vision to move away from file-centric processes and focus on delivering content in association with hardened person identities. The data streaming services are a combination of data delivery tools and connections to facilitate the seamless communication between different USCIS systems. Content Management Services does not directly connect to any USCIS systems and relies on the data streaming services to display information. USCIS uses data streaming services to integrate existing systems with new applications and support services. The integration with these data streaming services allows Content Management Services to share and receive information from other systems without adversely impacting the availability of Content Management Services.

Access to Digital Records in Content Management Services

Content Management Services is a dynamic and collaborative system that supports the management, creation, and modification of digital content through the user interface STACKS (not an acronym) or through an interconnected system. Through both access mechanisms, Content Management Services 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 Content Management Services to maintain in specific content repositories. The interconnected system is also able to retrieve the information from Content Management Services

---

[17] An Application Programming Interfaces is a set of defined rules that enable different applications to communicate with each other. It acts as an intermediary layer that processes data transfers between systems, letting companies open their application data and functionality to external third-party developers, business partners, and internal departments within their companies.

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR MYUSCIS ACCOUNT EXPERIENCE, DHS/USCIS/PIA-071 (2017 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

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

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS) ASYLUM DIVISION, DHS/USCIS/PIA-027(d) (2018), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[21] *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.

and display the information to the user through its respective user interface. For data accuracy and accountability, users' entries of and modifications to records in Content Management Services are logged and may be reviewed through an ad hoc, routine, or random audit process.

STACKS

STACKS is the latest USCIS enterprise viewing system for digital immigration record content in support of the USCIS transformation initiative. USCIS users will be able to view the immigration benefit request, supporting evidence, correspondence, as well as other internal or immigration benefit requestor submitted content that is considered part of the official immigration record. Transformation is an initiative to eliminate the creation of new paper immigration records when USCIS receives immigration benefit requests electronically, requests evidence electronically from immigration benefit requestors, and uses those digital records in the adjudication process.

Privacy Impact Analysis

Authorities and Other Requirements

The use of Content Management Services, STACKS, Scan on Demand Application, and Document Service Management System does not change the legal authorities that govern MiDAS. The following System of Records Notices (SORN) cover the personally identifiable information utilized in the MiDAS boundary:

DHS/USCIS-007 Benefits Information System,[22] which covers USCIS' collection, use, maintenance, dissemination, and storage of benefit request information, including case processing and decisional data not included in the A-File.

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,[23] which covers the paper and electronic copy A-File and/or Receipt File, supplemental forms, supplemental evidence, and identity history summaries but does not include all case processing and decisional data.

DHS/ALL-004 General Information Technology Access Account Records System (GITAARS),[24] which covers the collection, review, and maintenance of any logs, audits, or other security data regarding the use of DHS IT resources.

---

[22] *See* DHS/USCIS-007 Benefits Information System, 81 Fed. Reg. 72069 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[23] *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.
[24] *See* DHS/ALL-004 General Information Technology Access Account Records (GITAAR), 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

DHS/ALL-037 E-Authentication Records System of Records,[25] which allows DHS to collect, maintain, and retrieve records about individuals, including members of the public, who electronically authenticate their identities. The information in this system of records includes data collected by programs and applications for use DHS or a trusted third-party performs some or all the functions required to enroll, issue, and maintain a credential on DHS' behalf that can be used by an individual to electronically authenticate their identity to DHS systems.

Moreover, the collection of information for genealogy requests is subject to the Paperwork Reduction Act (PRA). USCIS obtained approval from the Office of Management and Budget (OMB) [(OMB Control No. 1615-0040)] for Form G-1041, *Genealogy Index Search Request*,[26] and Form G-1041A*, Genealogy Records Request*,[27] if requested by mail.

Characterization of the Information

The characterization of information requested or used by both the Genealogy Services Branch and the Office of Records Management from government agencies and member of the public requestors, and the subject of the search, has not changed with this MiDAS Privacy Impact Assessment Update.

The Scan on Demand Application database collects,[28] and temporarily stores for quality assurance, the following information in the process of digitizing immigration-related paper forms:

- Employee/requestor name;
- USCIS employee user ID;
- Name of requesting agency;
- A-Number; and
- File location.

The metadata saved in Content Management Services with every digitized A-File received from the Scan on Demand Application includes:

- A-Number;
- Name;

---

[25] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 Fed. Reg. 46857 (August 11, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[26] *See* Form G-1041, *Genealogy Index Search Request*, *available at* https://www.uscis.gov/g-1041.
[27] *See* Form G-1041A, *Genealogy Records Request*, *available at* https://www.uscis.gov/g-1041a.
[28] Scan on Demand Application does not "collect" information, but rather stores information for a short period of time, normally a few weeks, to give USCIS enough time to perform quality assurance checks, before sending for permanent storage to Content Management Services.

- Date of birth;
- Country of birth; and
- Receipt number.

Content Management Services serves as the repository of digital immigration-related content. As such, the digital content may take the form of electronic documents, records, images, videos, or other binary files containing information. The digital content within Content Management Services may include the following types of information:

- Immigration request forms;
- Supplemental documents in support of an immigration benefit 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);
- 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/Privacy Act 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:

- 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 (e.g., photographs and signatures from immigration benefit applicants);
- Enforcement supporting documents; and
- Other documents (e.g., naturalization certificates; tax returns; labor certifications; correspondence; court dispositions; interview notes).

The Document Service Management System only stores the information needed from USCIS employees and contractors to order the blank documents or produce form-use reports by offices for management purposes, and does not collect personally identifiable information from the public. Information collected from USCIS employees and contractors includes:

- Name;
- Approvers/endorser's name;
- Field office director's name (as applicable);
- USCIS email addresses; and
- Order tracking number tied to specific requestors.

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

Mitigation: This risk is mitigated. Content Management Services places responsibility for the accuracy and quality of information on each source system and their business and system managers. Content Management Services does not change data enroute to the receiving system other than to provide standardized formatting of the data, such as date and time formatting. Source systems depend on information provided directly from the subject person, such as an applicant, petitioner, or beneficiary via an immigration benefit request or other request for action.

Privacy Risk: There is a risk that the information maintained in Content Management Services and shared by MiDAS is inaccurate. As a result, USCIS will rely on inaccurate information 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 the 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 the immigration benefit or request 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 individual applicant, petitioner, or requestor is unaware, it would be provided to the immigration requestor in a Notice of Intent to Deny or Notice of Intent to Terminate, in an interview, or in similar processes, and the immigration requestor would have an opportunity to review and respond. For certain benefit types, after a final decision, USCIS may also permit requestors to correct information on USCIS issued documents if they believe or the information on the document is inaccurate.

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 Content Management Services using a unique personal identifier (e.g., A-Number, 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 Content Management Services are not inadvertently associated with the incorrect individual or benefit filing.

Uses of the Information

The uses of the information used and processed in MiDAS do not materially change with this Privacy Impact Assessment Update. USCIS retains these records for historical purposes, sharing with government agencies for mission-related purposes, and making them available to members of the public who are interested in obtaining the records for genealogical and other historical research.

Government agencies and members of the public use the immigration records obtained by USCIS for genealogical and other historical research. In many cases, USCIS is the only government agency that has certain historical records that provide the missing link for which genealogists or family historians search. USCIS will also provide this information to genealogists or family historians to assist in completing their search. The USCIS genealogy program only shares records of deceased subjects with members of the public. If a member of the public requestor requests historical immigration-related records containing information about living individuals, the Genealogy Services Branch will cancel the USCIS Genealogy Request, and the individual will be advised to submit a FOIA/Privacy Act request.

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

- Confirm identity using dates of birth, photos, or other biographic or biometric information;
- Confirm relationships using information found in birth, marriage, divorce, and/or adoption certificates;
- Confirm law enforcement actions using investigation reports, rap sheets;
- Confirm previous immigration benefit processing, including both approvals and denials; and
- Research customer inquiries and begin initial application review.

MiDAS users can access immigration case file information electronically stored in Content Management Services through the user interface STACKS, which allows USCIS, in the standard course of their immigration-related business, to access the files more rapidly and efficiently, and collaboratively use the files and mitigate the risk of losing the paper-based files. Content Management Services and the Scan on Demand Application eliminate the inefficiencies associated with paper records, such as slow, resource-intensive shipping, high risk of loss, and deterioration over time.

Privacy Risk: There is a risk that the information collected may be used for purposes that do not align with the USCIS mission.

Mitigation: This risk is mitigated. Members of the public who request information about deceased individuals may obtain the data and use it for their own intended purpose. If USCIS receives a request for an individual who is over 100 years of age, USCIS presumes they are deceased. Documentary evidence of the subject's death is required when USCIS receives a request regarding a subject born less than 100 years prior to the date of the request. Requestors must provide additional evidence including death records, published obituaries, published death notices, or published eulogies, church or bible records, photographs of gravestones, or copies of official documents relating to payment of death benefits. Government agencies can access information in MiDAS on both deceased and living subjects. For living individuals, USCIS only shares information when compatible with the purpose for collection, pursuant to one of the Privacy Act's statutory exceptions or pursuant to a routine use as outlined in the A-File, Index, and National File Tracking System of Records Notice and Benefits Information System System of Records Notice.

Privacy Risk: There is a risk that individuals who have legitimate access to MiDAS, Content Management Services, and the Scan on Demand Application could exceed their authority and use the data for unofficial purposes.

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

Notice

The notice provided to MiDAS requestors does not change with this Privacy Impact Assessment Update because the addition of the Scan on Demand Application and Document Service Management System to its security authorization boundary and the retrieval of requested digitized immigration-related information from the Content Management Services/STACKS, a USCIS data repository, does not impact MiDAS' privacy notice activities.

USCIS provides notice to individuals by providing a Privacy Notice on Form G-1041, *Genealogy Index Search Request*; Form G-1041A, *Genealogy Records Request*; and the Records Management Web Request site. The Privacy Notice provides the requestor with notice as to why USCIS is requesting the information, that their submission of the form is voluntary, how their information may be used, and the authority for collecting the information.

Data Retention by the Project

Information (data and electronic images) pertaining to correspondence with the public and government requestors is retained and disposed every six years in accordance with the NARA General Records Schedule 4.2, item 020, and General Records Schedule 6.5, item 010.

Information contained in MiDAS is retained and disposed of in accordance with the schedule, N1-566-06-2. These records are permanent and retained by USCIS for 100 years from the date of the individual's birth and therefore not subject to destruction. The Genealogy Case File and Historical Information Case File (for government requestors) is retained and disposed of in

accordance with schedules N1-566-12-01 and N1-566-12-02. These records are deleted and destroyed three years after the case is closed.

USCIS retains A-Files and Receipt Files in accordance with N1-566-08-11 and N1-85-96-01, respectively. N1-GRS-95-2, item 1c, governs the Scan on Demand Application database, which allows data within Scan on Demand Application to be deleted/destroyed when no longer needed for administrative, legal, audit, or other operational purposes.

Outputs sent to both the government agencies and member of the public requestors (e.g., acknowledgment letters, screen prints, response letters, responsive documents) are destroyed when no longer needed, in accordance with the General Records Schedule 4.3, item 30.

Privacy: There is a risk that MiDAS may retain information longer than is necessary to process requests or the Scan on Demand Application digitization efforts.

Mitigation: This risk is mitigated. USCIS is responsible for all personally identifiable information associated with MiDAS, and it therefore imposes strict requirements on vendors for safeguarding personally identifiable information data. This includes adherence to DHS 4300A Sensitive Systems Handbook,[29] which provides implementation criteria for the rigorous requirements mandated by DHS Information Security Program.

Information Sharing

This update does not materially change the information sharing as outlined in previous iterations of this Privacy Impact Assessment.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. If the individual is still living and would like to access their information, they may submit a FOIA or Privacy Act request to USCIS. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) may still obtain access to records consistent with the FOIA unless disclosure is prohibited by law or if the agency reasonably foresaw that disclosure would harm an interest protected by an exemption. U.S. citizens and lawful permanent residents may also file a Privacy Act request to access their information. If an individual would like to file a FOIA or Privacy Act request to view their USCIS record, the request can be mailed to the following address:

U.S. Citizenship and Immigration Services
National Records Center

[29] DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

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

Further information about FOIA and Privacy Act requests for USCIS records is available at http://www.uscis.gov.

The FOIA and Privacy Act request should contain the following information: name, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requestors must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. § 1746.

Persons not covered by the Privacy Act or Judicial Redress Act are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in their record received through FOIA they may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

Auditing and Accountability

This Privacy Impact Assessment update for MiDAS does not materially change the auditing and accountability posture of this system. USCIS ensures that the information is used in accordance with this Privacy Impact Assessment update by requiring training, policies, rules of behavior, and auditing and accountability practices. USCIS established access and security controls to mitigate privacy risks associated with authorized and unauthorized uses, namely misuse and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. USCIS tracks all user actions via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

All USCIS employees and contractors are required to complete annual privacy and security awareness training.

USCIS employs user-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know to perform their duties. As discussed above, for external agencies, USCIS determines compatibility prior to providing external agencies access to Office of Records Management Web Request site. Each user role is mapped to the set of system authorizations required to support the intended duties of the role. 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. The need-to-know and compatibility is determined by the respective responsibilities of USCIS or external user. Supervisors maintain

administrator privileges which allow them to add and remove users. USCIS audits the list of users annually.

Responsible Official

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

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
privacy@hq.dhs.gov