Privacy Impact Assessment Update
for the

Central Index System 2

DHS/USCIS/PIA-009(b)

December 17, 2018

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

<u>Reviewing Official</u>
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) maintains the Central Index System (CIS). CIS is a repository of electronic data that contains an index of basic data elements related to an individual as he or she passes through the immigration process. CIS contains information on the status of applicants and petitioners seeking immigrant and non-immigrant benefits, including: lawful permanent residents, naturalized citizens, United States border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). Recently USCIS migrated records from a legacy mainframe database to a cloud platform and renamed legacy CIS to CIS 2. CIS2 continues to look and function like the CIS mainframe application, with subtle formatting enhancements. USCIS is updating the CIS Privacy Impact Assessment (PIA) to assess the privacy risks associated with the changes to the storage and maintenance of personally identifiable information (PII) in this new cloud platform.

Overview

U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States and is responsible for processing petitions, applications, and other requests for immigration benefits. The Central Index System (CIS) was originally established to support the legacy Immigration and Naturalization Services (INS) records management needs to collect and disseminate biographic and historical information related to individuals during the immigration life cycle. CIS is now being fully used by Department of Homeland Security (DHS) components and other federal agencies pursuant to information sharing agreements and is maintained by USCIS. Due to system modernizations, USCIS recently renamed legacy CIS to CIS 2.

CIS 2 serves as a DHS-wide index system to track the location of case files, including Alien Files (A-File), and to maintain alien status and repository of information. CIS 2 contains information on the status of individuals, including lawful permanent residents, naturalized citizens, U.S. border crossers, apprehended aliens, aliens who have been issued employment authorizations, and other individuals of interest to DHS. CIS 2 provides information used for granting or denying benefits and capturing subsequent status changes; documenting chain of custody for enforcement purposes; keeping track of immigrant statistics; and control and account of record keeping services in accordance with the Code of Federal Regulations (CFR) to certify the existence or non-existence of records.

CIS 2 is a repository of electronic data that summarizes the history of an immigrant in the adjudication process. Information contained within CIS 2 is used for immigration benefit determination and for immigration law enforcement operations by USCIS, U.S. Immigration and

Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP) and may be used by federal, state, and local benefit programs, and by federal, state, and local law enforcement entities.

Reason for the PIA Update

On December 9, 2010, the Office for Management and Budget (OMB) released a "25 Point Implementation Plan to Reform Federal Information Technology Management," which required the Federal Government to immediately shift to a "Cloud First" policy.[1] The three-part OMB strategy on cloud technology revolves around using commercial cloud technologies when feasible, launching private government clouds, and utilizing regional clouds with state and local governments when appropriate.

When evaluating options for new IT deployments, OMB requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment.

USCIS is undergoing a system modernization effort to align with the OMB "Cloud First" policy to improve business operations. Legacy CIS was built using a dated mainframe database system. USCIS migrated the CIS mainframe application to Amazon Web Service (AWS) East/West and renamed the system to CIS 2. There were no changes to the collection and use of PII in CIS 2 from the previous legacy system. CIS 2, a modernized cloud-based application, absorbed legacy CIS mainframe functionality and system interfaces. All existing CIS records were extracted from the mainframe database and transferred to the new CIS cloud environment.

CIS 2 records are maintained in AWS, which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[2] AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[3] USCIS requires the AWS to segregate CIS 2 data from all other third-party

[1] 25 Point Implementation Plan to Reform Federal Information Technology Management (December 9, 2010), *available at* https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

[2] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.

[3] For more information, *see* https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.

data to preserve the quality and integrity of the data. FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. As a part of the USCIS Ongoing Authorization program, any identified vulnerabilities are reviewed on a monthly basis and scheduled for remediation. In addition, Information System Security Officers are required to perform continuous testing of Management and Operational controls based on the Ongoing Authorization frequencies and requirements.

This CIS 2 PIA update is limited to the migration from the mainframe to the cloud platform, which offers a flexible and adaptable Information Technology infrastructure. USCIS plans to enhance CIS 2 with future system modifications, which may address and mitigate the privacy risks detailed below. USCIS will update this PIA prior to implementing any new system enhancements.

Privacy Impact Analysis

Authorities and Other Requirements

The authority to collect information in the CIS is set forth in the Immigration and Nationality Act, 8 U.S.C. §§ 1101, 1103, 1304, et seq., and implementing regulations found in 8 CFR. There is no change in legal authority associated with the transition to CIS 2.The Alien File, Index, and National File Tracking System of Records continues to cover the collection, use, and maintenance for information in CIS 2.[4]

CIS 2 is a major application that is currently undergoing the Authority to Operate (ATO) process. Upon completion, CIS 2 will be accepted into the Ongoing Authorization program. Ongoing Authorization requires CIS 2 to be reviewed on a monthly basis and maintain its security and privacy posture to maintain its ATO.

The National Archives and Records Administration (NARA) approved the CIS 2 retention schedule N1-566-10-01 on November 05, 2009. According to this retention schedule, which is unaffected by the transition to CIS 2, records are permanent and USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

CIS 2 is not subject to Paperwork Reduction Act (PRA) requirements.

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

Characterization of the Information

This update does not impact the collection of information in CIS. USCIS continues to collect and maintain the information outlined in the DHS/USCIS/PIA-009(a) CIS, published on April 7, 2017.

Privacy Risk: There is a risk that the information in CIS 2 may be inaccurate due to manual entry of data.

Mitigation: Only authorized USCIS Records staff have the ability to add or edit data and create Alien Numbers (A-Numbers) electronically. CIS 2 validates data entry through program coding to mitigate or prevent inconsistencies in applicant data and in decision processing entries (e.g., the system rejects 00/00/00 birthdates). Validation checks are performed when the data is entered and verification of the data is performed by subsequent processing and cross-checked with other sources. Data entry personnel are provided with the opportunity to review and edit information prior to and after their submission.

Privacy Risk: There is a risk that USCIS, DHS, and other external users may update CIS 2 with incorrect information.

Mitigation: USCIS partially mitigated this risk. Only a few USCIS employees are able to make edits directly in CIS 2. Most users of CIS 2 only have read-only access through CIS 2 directly or through the Person Centric Query System.[5] Those users must go to the source system to make changes to data that would reflect in CIS 2 when the data refreshes on a nightly basis. CIS 2 is unable to validate whether the changes made in the source system are accurate.

Privacy Risk: There is a privacy risk that an individual was issued more than one A-Number, resulting in multiple records in CIS 2.

Mitigation: This risk is partially mitigated. The A-Number is a major key to locating data in CIS 2. USCIS may identify that more than one A-File was issued to an individuals. In the event that an individual was inadvertently issued more than one A-Number, USCIS lists all A-Numbers for subjects who may have had multiple A-Numbers assigned in their CIS 2 record. USCIS reviews all of the multiple A-Numbers identified during the CIS check. USCIS consolidates all A-Numbers in CIS 2 by identifying primary and secondary A-Numbers. A primary A-Number is the number currently assigned to the surviving physical paper file and it is the first number listed in CIS 2. A secondary A-Number(s) are those that been consolidated into the primary A-Number, and are listed below the primary number.

[5] See DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), available at www.dhs.gov/privacy.

Uses of the Information

This update does not impact the uses of CIS 2 records. CIS 2 continues to serve as a repository of electronic data that contains an index of basic data elements related to an individual as he or she passes through the immigration process. CIS 2 also continues to provide a searchable index of A-Files and to support the location and transfer of A-Files among DHS personnel and offices as needed in support of immigration benefits and enforcement actions.

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

Mitigation: The risk is partially mitigated. To ensure the information is used consistently with the purposes of the original collection, USCIS monitors audit logs to ensure users are only accessing information related to their job functions. Prior to accessing CIS 2, each DHS user must sign a user access agreement that outlines the appropriate rules of behavior tailored to CIS 2. External agency representatives viewing the data must sign a non-disclosure agreement, which outlines the limits and restrictions regarding use of the data. Agencies requesting access to information/files are required to send a memorandum on official letterhead, signed by the local director, with an accreditation list identifying the names of those individuals that have been authorized to review information contained within USCIS records/systems.

USCIS implements disciplinary rules to ensure the appropriate use of the system. USCIS reminds employees accessing the system that the system may be monitored for improper use and illicit activity, and the penalties for non-compliance, through a warning banner that reiterates the appropriate uses of the system. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This process acts as a deterrent to unauthorized activity.

Privacy Risk: There is a risk that unauthorized users may gain access to CIS 2.

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 personnel who have a need to know. CIS 2 is a cloud-based application that is only available through the DHS USCIS network. All access is secured through access controls requiring PIV card. Authorized employees must use their issued credentials, also known as PIV cards, to gain access to CIS 2. Individuals who do not require access to CIS 2 will not be able to access CIS 2 through their PIV card. Access to the system via PIV card is consistent with the National Institute of Standards and Technology 800-63 Level 4-assurance of the user's identity.

Privacy Risk: There is a risk that USCIS may provide unauthorized individuals access to CIS.

Mitigation: Since the formation of DHS, read-only access to information contained in legacy CIS (and now CIS 2) has been provided to the following three components: 1) CBP, for border and inspection process; 2) USCIS, for immigration benefit adjudication process; and 3) ICE, for investigatory, deportation, and immigration court functions. Information is accessible by all three components so that they may perform their mission requirements. Officers have read-only access, and include adjudications officers who review applications and assign benefits, and enforcement officers who encounter individuals at the ports of entry, borders, and interior of the United States, and must verify the status of those individuals. Only specific authorized USCIS Records users have the ability to add or edit data and create and verify A-Numbers electronically. USCIS is careful to only share data with other DHS components who need to know the information. Only USCIS internal users, System Administrators, and Data Base Administrators have write and modify access to the CIS 2 application and CIS 2 database files.

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

Mitigation: USCIS has partially mitigated this risk. CIS 2 includes an alert message to indicate that an individual is protected by 8 U.S.C. § 1367. The release will help users comply with 8 U.S.C § 1367(a), which prohibits DHS from making unauthorized disclosures of information related to certain protected classes of aliens, including applicants and recipients of T (victims of human trafficking) and U (victims of criminal activity) visas, and relief under the Violence Against Women Act of 1994 (VAWA). This enhancement also makes CIS 2 users immediately aware that they are displaying a record relating to a protected individual and that specific procedure regarding the disclosure and use apply. Any record in CIS 2 that displays this banner must be handled as Section 1367 Information in accordance with USCIS policy.

Notice

This PIA update provides general notice to the public by describing the changes to information storage and maintenance practices by USCIS as data is migrated to the AWS public cloud platform. USCIS continues to provide notice to individuals through Privacy Notices on benefit request forms and the Alien File, Index, and National File Tracking System SORN.[6]

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not have notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. USCIS is providing notice through the publication of this PIA. USCIS provides notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice that the information may be stored in a cloud-based system at the time of collection. Regardless of storage location of records, the

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

records in CIS 2 are governed by the USCIS' collection, use, and dissemination of their information.

Data Retention by the project

This update does not change the length of time data is retained in CIS 2. USCIS continues to adhere to the NARA-approved retention schedule N1-566-10-01 for CIS 2. The records in CIS 2 are designated as permanent records and USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

Information Sharing

This update does not impact information sharing with internal or external entities. USCIS continues to share information with internal and external entities as outlined in DHS/USCIS/PIA-009(a) CIS, published on April 7, 2017.

Redress

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

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

Persons not covered by the Privacy Act or JRA 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

Auditing and Accountability

USCIS ensures that practices stated in this PIA update comply with internal federal, DHS, and USCIS policies, including the USCIS privacy policies, Standard Operating Procedures, orientation and training, rules of behavior, and auditing and accountability procedures. CIS 2 records are maintained in the AWS platform, which is FedRAMP-approved and authorized to host PII. FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. In addition, USCIS requires CIS 2 to undergo the security assessment process to verify adherence to DHS privacy and security requirements. Though the security assessment process, USCIS validates technical and security controls to preserve the confidentiality, integrity, and availability of the data.

USCIS replaced the legacy mainframe with a cloud-based platform, resulting in USCIS updating the system access request process as part of this system modernization. Previously, the process to request and obtain access to the USCIS mainframe systems, including CIS, was facilitated through Password Issuance and Control System (PICS). The PICS request process was operated by ICE. PICS automated the process of requesting, issuing, and managing logon credentials that were required to gain access to certain ICE and USCIS information mainframe systems. PICS was fully decommissioned and all functions previously handled by PICS are now completed through the USCIS myAccess portal.

The myAccess portal replaces the legacy account approval process provided by ICE PICS. 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, including CIS. All internal and external access requests to CIS are governed by USCIS through myAccess. Any new user requiring access to the CIS 2 must create a profile and submit an access request in myAccess.

The Immigration Records and Identity Services Directorate (IRIS) Records Division reviews and approves all incoming internal and external access requests to CIS 2 data through myAccess. The Records Division coordinates the review with the proper authorizing officials such as the USCIS Privacy Officer, Chief of Information Security Officer, and Office of Chief Counsel. During this coordinated review, the authorizing authorities review the request to ensure access and use of the system is consistent with the legal authority and uses. Information contained within CIS 2 is used for immigration benefit determination by USCIS and for immigration law enforcement operations by ICE and CBP, and CIS 2 may also be accessed by external federal entities. For external entities, in addition to the Records Division review, an information sharing agreement between USCIS and the third party and appropriate privacy compliance documentation are executed prior to such third party entity being provided access to CIS 2.

USCIS also implements role based access controls for internal and external users, which give each user a standard role and a standard set of permissions to prevent the user from accessing anything outside their assigned role. Individuals granted access to CIS 2 use their government-issued Personal Identity Verification (PIV) card to access the CIS 2 application. A PIV card is a United States federal smart card that contains the necessary data for the cardholder to be granted access to federal facilities and information systems, and assure appropriate levels of security for all applicable federal applications. These technical and security controls limit access to USCIS users and mitigate privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify 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.

Privacy Risk: There is a risk to security because CIS 2 records are stored on third-party servers, which may not have been assessed by USCIS security compliance personnel to ensure compliance with federal IT security requirements.

Mitigation: USCIS cloud service providers must be FedRAMP certified. By using FedRAMP-certified providers, DHS leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance.

All contracted cloud service providers must follow DHS privacy and security policy requirements. Before using AWS, USCIS verified through a risk assessment that AWS met all DHS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the USCIS Federal Information Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance. As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

Privacy Risk: There is a risk that CIS 2 records can be accessed by unauthorized personnel since CIS 2 now resides in AWS, a public cloud.

Mitigation: This risk is mitigated. Although CIS 2 operates in a public cloud, CIS 2 is separated from other public cloud customers. CIS 2 operates in a Virtual Private Cloud, which is a private component to the public cloud. USCIS controls access to the systems within the cloud, not AWS.

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 CIS 2 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.[7]

Responsible Official

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

Approval Signature

[Original signed and on file with the DHS Privacy Office]

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

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