Privacy Impact Assessment
for the

Central Index System

June 22, 2007

Contact Point

Elizabeth Gaffin
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security United States Citizenship and Immigration Services maintains the Central Index System (CIS), a database system originally developed by the legacy Immigration and Naturalization Service. CIS contains information on the status of 57 million applicants/petitioners seeking immigration benefits to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., 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). This PIA addresses the current status of CIS, and will be updated accordingly as additional USCIS applications and system functionalities are added to CIS.

Introduction

Background

CIS replaced the old Master Index System in 1985 to support a legacy INS records management need to collect and disseminate automated biographic and historical information on the status of 57 million applicants/petitioners (applicants) seeking immigration benefits to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., 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 INA. CIS currently serves as a DHS-wide index, maintains immigrant and non-immigrant status information on alien and other individuals subject to the provisions of the INA, and tracks the location of paper case files, known as Alien Files ("A-files"), in local file control offices (FCO). Information contained within CIS is used for immigration benefit determination, and for immigration law enforcement operations by USCIS, Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP). Information contained within CIS is also used by federal, state and local benefit bestowing programs, and by federal, state and local law enforcement entities. CIS interfaces with over 20 internal DHS data systems and a small number of external governmental entities.

CIS is available to any DHS personnel with appropriate security authorization and a need for information through any authorized DHS IT device connected to the DHS network. CIS provides a central repository of data that allows the USCIS Records Division to assist other entities inside and outside of DHS that require information contained within CIS to respond to legal and governmental needs, such as subpoenas and Congressional oversight committee requests.

Transaction Record Keeping System (TRKS) was created in 1993 as a subsystem of CIS. TRKS

provides security and audit information to a limited number of authorized USCIS Records Division users, and captures any modifications made to an Alien Number ("A-Number") by a user or system update through an online query.

DHS assigns an individual a unique identification number that is known as an A-Number when the individual applies for immigration related benefits, or is the subject of a law enforcement action. A-Numbers may also be issued by the Department of State (DOS) in limited circumstances overseas for the issuance of visas. In order to collect and maintain hard copy information relating to individuals who have been issued A-Numbers, DHS creates an Alien Files ("A-File"), which are paper-based files. An A-File is the series of records that USCIS maintains on individuals under the purview of the INA and relevant regulations, which documents the history of their interaction with DHS as required by law. USCIS is the designated custodian of A-Files for all of DHS, and thus, keeps A-Files in physical folders labeled with barcodes that are indexed electronically in CIS. Paper case A-Files are currently being digitized in order to provide simultaneous electronic access in the event multiple entities require the file.

After a paper A-File is generated for a person, USCIS Records Personnel electronically create the A-File in CIS capturing eight required data fields which include, A-Number, first name, last name, date of birth, File Control Office, Country of Birth, Date File Opened, Class of Admission. Only Records Personnel and/or Records Contract Staff are designated and trained to perform the electronic creation of an entry in CIS and or an electronic A-File. The A-File may include information on U.S. Citizens if the Alien's immigration status is derived or acquired based on his or her relationship to a U.S. citizen. CIS may contain additional information.

As a general matter, CIS does not create a file on a native born U.S Citizen, and thus, information pertaining to native born citizens is not normally accessible or available by querying CIS. However, in some rare instances, a U.S. Citizen may have committed an immigration law violation and/or is the subject of an investigation related to an immigration violation. In such circumstance an A-File will be created. In addition, in the event that a person (native born or naturalized) decides that he or she does not want to be a U.S. citizen, he or she may formally renounce his or her citizenship through DOS. DOS sends a Certificate of Loss of Nationality to USCIS to be filed in an A-File created for this purpose.

The A-File and CIS contain information obtained from the following types of individuals:

- Individuals who have a valid immigrant status
- Individuals applying for immigration benefits
- Individuals who break immigration laws or who are suspected of breaking immigration laws
- Individuals who have derived or acquired citizenship

- Individuals who have relinquished their citizenship
- Asylees and refugees

Historic Files

USCIS maintains A-File information captured prior to 1940 in historical files that are contained on microfiche, microfilm, index cards, and in certificate files. These historic records have moved into the Microfilm Index Digitization Application System (MiDAS), designed to capture the information from these older decaying types of media. Only the information contained in naturalization certificate files contains the eight data elements required by CIS to allow it to be created electronically in the system so the file may be sent to another location for review if requested. This is the only time that information contained in MiDAS will also be in CIS.

Technology

CIS is a searchable mainframe production application located and maintained at a Department of Justice (DOJ) data center. Authorized DHS personnel with a need to know the information access these applications usually through Wide Area Network (WAN) and Transmission Control Protocol/Internet Protocol (TCP/IP) log-in connections from locations throughout the U.S. and overseas. CIS also interfaces with other DHS databases to provide comprehensive data necessary for DHS operations.

CIS receives data uploaded on a nightly basis from the following internal DHS systems and external data systems:

Internal Systems – USCIS –

- CARD — Alien Registration Card / Border Crossing Card Interface (USCIS)
- CLAIMS3 — Computer-Linked Application Information Management System 3 (USCIS)
- CLAIMS4 — Computer-Linked Application Information Management System 4 (USCIS)
- EADS — Employment Authorization Documentation System (USCIS)
- MFAS — Marriage Fraud Act Amendment System
- RNACS — Re-designed Naturalization Automated Casework System (USCIS)
- NFTS — National File Tracking System (USCIS)
- RAFACS — Receipt and Alien File Accountability and Control System (USCIS)
- RAPS — Refugee Asylum and Parole System (USCIS)

- TRKS Transaction Record Keeping System (USCIS)
- VIS Verification Information System (USCIS)

Other Internal DHS Systems

- DACS Deportable Alien Control System (ICE)

External Systems

- VP Visa Packet (DOS) via the CBP Datashare Initiative
- EOIR Executive Office of Immigration Review (DOJ)
- DSI Data Sharing Initiative (DOS)
- SSA Social Security Administration Enumeration (SSA)

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

There are eight mandatory fields for A-File data in CIS: A-Number, first name, last name, date of birth, class of admission, country of birth, creation date of file, and the FCO (local file control offices) where the file is located. CIS may contain the following additional data elements:

- Social Security Number (or other unique identifying number issued by a governmental entity) if available. SSN is not a mandatory data element and is only captured in CIS if available in the A-File.
- Fingerprint CD Number - This is a legacy data element that was collected from paper fingerprint cards and entered manually in the system. DHS no longer collects or uses this data element for adjudication purposes.
- Derivative Citizenship Number (DA)
- Naturalization Certificate Number (C-Number)
- Mother's Name
- Father's Name
- Also known as (AKA) Last and First Name
- Port of Entry (POE) at which the individual entered the country
- Driver's License Number , if available

Immigration court information and deportation information can also be found in the system.

Information on an individual can be retrieved by the following data elements:

- Alien Number
- Name and/or alias
- Social Security Number (or other number originated by a government that can be used to identify an individual) or,
- Naturalization Certificate Number (C-Number)

1.2 From whom is information collected?

Much of the data contained in CIS is obtained directly from the individual requesting benefits under the Immigration and Naturalization Act, either filed with DHS or with DOS on an OMB approved form. Other information may come from records resulting from enforcement operations where a person is apprehended at the border, internally in the United States, or when a person has a warrant for deportation. Information is gathered from enforcement forms within ICE and CBP, then used to create physical A-Files, and later followed by records personnel creating the electronic A-Number in CIS.

1.3 Why is the information being collected?

The information is collected so that DHS can maintain an electronic retrieval system containing information related to immigration status/class of admission on aliens and other individuals under the purview of the INA.

CIS supports DHS informational needs by providing the following major capabilities:

- Enabling personnel located in DHS field offices, ports of entry, and examination and inspection sites to promptly access accurate biographical and class of admission/status information on individuals seeking legal entry to or residence in the United States, thus ensuring proper entry and granting of benefits to eligible individuals.
- Assisting DHS in the identification of individuals who violate the terms of their stay, who enter the United States illegally, or who are otherwise not entitled to entry or benefits.
- Providing DHS officials with timely access to appropriate A-Files by identifying the location of hard copy A-Files on individuals of interest to DHS.
- Serving as a starting point for a system that will ultimately move data without the need to move paper A-Files.

- Providing statistical reports to DHS, other government agencies, and certain public interest groups.
- Enabling DHS to monitor areas of progress and problems within USCIS that require attention or action.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The authority to collect information in the CIS is set forth in the Immigration and Nationality Act, 8 USC §§1101, 1103, 1304 et seq., and implementing regulations found in 8 CFR.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

CIS requires eight data elements in order to create and electronically record in the system. These include: A-Number, date file opened, class of admission code, first name, last name, date of birth, country of birth, and file control office (denotes physical location of the A-File).

Other fields, such as SSN, mother's name, father's name, are populated only if an applicant/petitioner provides the information on a form submitted to USCIS, ICE, or CBP, and is included in the physical A-File.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

CIS serves as an initial screening process to provide a brief overview of a person's basic information (described in Section 1) to determine if there is a need to request the physical file. This includes the ability to ascertain an individual's current immigration status (class of admission) and prior status (class of admission).

CIS maintains this basic information for both benefit bestowing agencies and by law enforcement to determine if, based on their class of admission code and other data elements, an individual is eligible for processing of a benefit, or should be detained and/or investigated for enforcement reasons, in which case the user would request the physical A-File. The information regarding class of admission in CIS is derived from DHS's administrative actions related to a person's initial application/petition or apprehension. Any updates of the class of admission are sent via other systems described in Section 1 and are based on information input from forms or petitions.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "data mining")?

No, CIS does not analyze data for the purpose of identifying unknown areas of concern.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information entered/created within CIS is verified to ensure that duplicative information does not already exist. The physical creation of a new file can be prepared by several authorized individuals; however, the electronic creation and input of data can only be accomplished by USCIS Records Personnel or USCIS Records Contract Staff who are trained and designated to perform this function. An A-File is not considered to be created until it has been electronically created within CIS. This creation requires that one individual enters the data while another individual verifies the accuracy of the information derived from the physical A-File. The verification process must be completed within 48 hours or the information will be deleted from the system. Any information uploaded from another system undergoes a series of automated data checks before being added to the system.

CIS generates error reports in the event a record is rejected due to faulty, incomplete or incorrect data. The USCIS File Control Office that entered the uploaded information will be notified of the error and must address the noted deficiency prior to re-sending the information.

USCIS developed procedures for updating the information if users notice inconsistencies between the paper A-File and CIS. Only a limited number of authorized USCIS Records Personnel may update the system accordingly.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy Risk – Inappropriate use of the information

Mitigation - Only personnel with the proper security clearance and a need for the information will be granted access to CIS. The system administrator is responsible for granting the appropriate level of access. All USCIS employees and external government users will be properly trained on the use and release of information in accordance with agency policies, procedures, regulations, and guidance contained within the DHS/USCIS 001 A-File/CIS SORN, 72 FR 1755. In addition, USCIS personnel are required to take annual computer security awareness training.

With respect to access to information by other government requesters, USCIS entered into a number of MOUs for the sharing of information contained within CIS and its "feeder systems." These documents dictate the terms and conditions for the release of relevant information as well as the appropriate use and safeguarding of all Personally Identifiable Information (PII). In the event there is the need for additional information sharing, USCIS will enter into additional MOUs that will contain specific requirements of the receiving entity relating to the safeguarding of PII.

Privacy Risk: Data Quality

Mitigation: USCIS has a number of procedures in place to check the data accuracy of information coming into CIS, including division of job duties to ensure that an A-File is accurately and only once created in CIS. Authorized USCIS Records personnel have the ability to correct inaccuracies brought to their attention internally, as well as by members of the public. Individuals may request the correction of information contained within their files by submitting a Privacy Act request. For more information see Section 7.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

USCIS follows the data retention and destruction policies as documented in DHS/USCIS-001 CIS/A-File SORN published January 16, 2007, in the Federal Register, Volume 72, page 1755. In particular:

- "A-File records are retained for 75 years from the date the file is retired to the Federal Records Center or date of last action (whichever is earlier) and then destroyed." USCIS is working with NARA for A-File information that will ultimately be made permanent records because of the historical value of the information. Consequently, data deletion will not occur.
- "C-file records are to be destroyed 100 years from March 31, 1956."
- Automated master index records are permanent and will be transferred to NARA.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

NC1-85-80-5, dated August 22, 1980

"Destroy [A-Files] seventy-five years from the date the file is retired to the Federal Records Center or seventy-five years from the date of last action, whichever is earlier."

N1-566-06-1, dated May 30, 2006

"Inputs, outputs, master files, and documentation, and electronic mail and word processing associated with an electronic information system used to conduct background checks on applicants/petitioners seeking benefits under the Immigration and Nationality Act. The agency proposes a 75 year retention for the master files. Disposition Schedule, N1-566-06-1, is pending approval from NARA.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

All data and electronic images are being retained for the indicated periods to fulfill the business requirements of DHS, which includes adjudication of decisions, law enforcement uses, protection of national security, responding to requests within DHS, as well as those requests from other government agencies requiring historical and/or biographical information on the individuals of interest. The information is retained for the specified period because the relationship between USCIS and the individual may span an individual's lifetime.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Since the formation of DHS, Read-Only access to information contained in CIS 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.

This information is also shared with other components within DHS on a case-by-case basis responsible for law enforcement intelligence activities.

4.2 For each organization, what information is shared and for what purpose?

All information in the system that is shared in DHS serves as an initial screening process to provide a quick look at a person's basic information (described in Section 1) to determine if there is a need to request the physical file. This includes looking at the current status (class of admission) and

prior status (class of admission). The basic information in CIS is used by both law enforcement and benefits bestowing operations to determine if, based on their class of admission code and other data elements, an individual is eligible for an immigration related benefit, or should be detained and/or investigated for enforcement reasons, in which case the government user would request the physical A-File. The information regarding class of admission in CIS is derived from a person's initial application/petition or apprehension. Any updates of the class of admission are sent via other systems described in Section 1 and are based on information input from forms or petitions.

4.3 How is the information transmitted or disclosed?

Capabilities exist to transfer information either electronically or via paper (i.e., e-mail, disk, fax, telephone, or mail). The transfer of data by portable media is accomplished in accordance with OMB Memorandum 06-16.

4.4 Privacy Impact Analysis:

The primary risk is unauthorized access to, or disclosure of, information contained with the system.

Information in this system is safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. This adheres to requirements of the DHS Information Technology Security Programs Handbook to include the issuance and use of password protection identification features. All internal components are mandated by DHS to comply with DHS' Sensitive System Security guidelines.

USCIS, ICE, and CBP are trained on how to interpret and use immigration information. USCIS, ICE or CBP will explain the meaning of information contained within CIS to non-immigration trained personnel in other DHS agencies prior to the dissemination of immigration related information contained within CIS.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

"Read only" access to CIS is provided to specific employees at federal agencies with whom USCIS has a signed MOU, such as Department of State (DOS), Social Security Administration (SSA), Office of Personnel Management (OPM), and Department of Justice (DOJ), specifically the Federal Bureau of Investigation.

Information contained within CIS may be shared with outside entities through other means. For example, CIS information is shared through the Verification and Information System (VIS)[1] for employment eligibility determinations as well as to assist other federal state and local governmental agencies in their determination as to whether an individual is eligible for a governmental benefit.

In addition, CIS information may be accessed by contacting DHS personnel at the ICE Law Enforcement Center when an NCIC request is received from state or local police.

5.2 What information is shared and for what purpose?

Information in CIS is used on a daily basis by DHS operational components, as well as by various federal and state entitlement and law enforcement programs. Information contained within CIS may be shared with DOS and SSA for benefit determinations, OPM for federal personnel purposes, and FBI and DOJ for law enforcement and prosecutions.

People with read-only access can view the history of the change in Class of Admission over a period of time.

5.3 How is the information transmitted or disclosed?

All users have read-only access to all of the information; however, ad-hoc transfers capabilities exist to transfer information either through encrypted electronic transmission or via paper (i.e., e-mail, disk, fax, telephone, or mail), if needed by contacting the USCIS Headquarters Records Division CIS project manager. Only the CIS contractor has the capability to provide this information at the direction of the authorized CIS project manager. Typically, this type of information is a result of a General Accounting Office (GAO) request.

DHS personnel with immigration expertise may also provide information contained in the system to external organizations who meet criteria outlined in the USCIS Records Operation Handbook, which states that it must be for the purpose of law enforcement or a routine use as described by the DHS/USCIS – 001 A-File and CIS System of Records Notice for the type of record requested.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

USCIS has entered into a number of MOUs with various agencies such as DOJ/FBI, OPM, DOS and SSA to share information contained within CIS and its feeder systems. These documents dictate the

[1] Verification Information System (VIS) Privacy Impact Assessment was issued on April 2, 2007. See www.dhs.gov/privacy under PIA for further information.

terms and conditions for the release of relevant information, as well as, the appropriate use and safeguarding of all PII. It is anticipated that USCIS will enter into additional MOUs in the future. The terms and conditions for the sharing of information with other governmental agencies are also provided for in the DHS/USCIS-001 Central Index/A-File SORN, 72 FR 1755.

5.5 How is the shared information secured by the recipient?

The handling of information shared with other agencies is governed by the terms and conditions set forth in the related MOUs, the DHS/USCIS-001 Central Index/A-File's SORN, 72 FR 1755, DHS-2006-0081, and in OMB guidance pertaining to the Safeguarding of PII.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No specific training is required of users external to DHS prior to being granted access to information. However, Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, "Safeguarding Personally Identifiable Information", dated June 23, 2006, which sets forth the standards for the handling and safeguarding of personally identifiable information. Contractors must sign non-disclosure agreements that dictate the confidentiality afforded to any accessed PII. External users are provided a CIS Quick Reference Guide on CD for use and facilitation of the information displayed in the system.

USCIS, ICE, and CBP are trained on how to interpret and use immigration information through the use of web-based system training, INA training, and other miscellaneous on-the-job training received per their specific role. USCIS, ICE or CBP will explain the meaning of information contained within CIS to non-immigration trained personnel in other DHS agencies prior to the dissemination of immigration related information contained within CIS. Information contained within CIS may be shared with outside entities through other means. For example, CIS information is shared through the Verification and Information System (VIS)[2] for employment eligibility determinations as well as to assist other federal state and local governmental agencies in determination for whether an individual is eligible for a governmental benefit. VIS shows a person's eligibility to work by translating the person's Class of Admission code in CIS into a statement of legally able to work or not.

In addition, CIS information may be accessed by contacting DHS personnel at the ICE Law Enforcement Center when an NCIC request is received from state or local police.

[2] Verification Information System (VIS) Privacy Impact Assessment was issued on April 2, 2007. See www.dhs.gov/privacy under PIA for further information.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: Unauthorized access to information or unlawful disclosure

Mitigation: The primary risk is unauthorized access to or disclosure of information contained in A-Files. To mitigate the risk, Records Division personnel strictly control the process of data sharing. As noted in 5.4, 5.5 and 5.6 above, a representative must be authorized to gain access to information contained within CIS. Only relevant portions of the A-File are provided. Non Government representatives viewing the data must sign a non-disclosure, 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. The risks are mitigated by provisions set forth in MOUs with the federal government agencies, and mandated annual security awareness training similar to training for USCIS employees.

Privacy Risk: Information security

Mitigation: USCIS has adopted the following information security practices to ensure information security: Federal agencies are located in buildings with controlled access by security guards or authorized contractors for the government. Individuals gaining access to premises are required to have official identification. Information in this system is also safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards include restricting access to authorized personnel who have a need-to-know. CIS is maintained at the DOJ Data Center (Dallas). Physical controls of the facility (e.g., guards, locks, etc.) have been implemented to prevent entry by unauthorized entities. Users are required to take mandatory Federal Computer Security Awareness training annually. Finally, CIS does not contain classified information.

Privacy Risk: Inappropriate Use of Information (Social Security number, A-Number, etc.)

Mitigation: USCIS only provides access to the system for to individuals who have a specific need to know access for the purpose of their job. Users must meet security training requirements. 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 authorized to review information contained within USCIS records/systems. The risks are also mitigated by provisions set forth in MOUs with the federal government agencies and by requiring mandated annual security awareness training similar to training for USCIS employees.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

A System of Records Notice (SORN) for the Alien File (A-File) and Central Index System (CIS) was last published January 16, 2007 in the Federal Register, Volume 72, pages 1755-1759 CIS.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes, applicants/petitioners can decline to provide information. However, the information contained in CIS is requested from immigration benefit applicants and petitioners to assist in the adjudication process. If the applicant does not wish to provide the information that is stored in the A-File, his/her request for immigration benefits may be denied.

In instances where the A-File is created for other purposes (e.g., enforcement, investigations), information may not be collected directly from the individual, and thus, the individual may not have an opportunity to decline to provide information contained within the A-File.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

An applicant provides consent by virtue of applying for a USCIS benefit. Many OMB approved application/petition requests for immigration related benefits contain the following statements, asking the applicant to provide DHS with the written authority to release information provided by the applicant to assist in the determination of eligibility for the requested benefit:

YOUR CERTIFICATION: I certify, under penalty of perjury under the laws of the United States of America, that the foregoing is true and correct. Furthermore, I authorize the release of any information from my records that U.S. Citizenship and immigration Services need to determine eligibility for the benefit that I am seeking.

For A-Files created for other purposes (e.g., enforcement, investigations), the individual does not consent to particular uses of the information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The extent of notice and opportunity to provide informed consent varies based on the particular purpose associated with the original collection of the information. In most cases, notice is provided when the applicant fills out the form or application for benefits. See Section 6.3. In the law enforcement or national security contexts, notice or opportunity to consent would compromise the ability of the agencies to perform their mission. In cases such as these, notice and consent may not be available.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The process for gaining access to one's information in an A-File is the same regardless of how it is stored (digital or paper). All requests for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals seeking information pertaining to them are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, provide the A-File number and/or the full name, date and place of birth, and notarized signature of the individual who is the subject of the record, and any other information which may assist in identifying and locating the record, and a return address. For convenience, Form G-639, FOIA/PA Request, may be obtained from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS website, located at www.uscis.gov.

An individual that would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services

National Records Center

FOIA/PA Office

P.O. Box 648010

Lee's Summit, MO 64064-8010

7.2 What are the procedures for correcting erroneous information?

Individuals may direct all requests to contest or amend information to the FOIA/PA Office at USCIS. They must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment thereof. Clearly mark the envelope "Privacy Act Amendment." The record must be identified in the same manner as described for making a request for access. Additionally, individuals may have an opportunity to correct their data during interviews when they visit a DHS district office, with supporting documentation in hand, and speak with an Immigration Information Officer (IIO), who can implement the change within the system, but only after ensuring the individual has the appropriate documentation that indicates there is an error. USCIS then corrects its systems, including auxiliary systems.

7.3 How are individuals notified of the procedures for correcting their information?

The FOIA/PA Officer at USCIS will notify the requester that information pertaining to them within the system has been corrected, but only after receiving a request to contest or amend information within CIS. The information is corrected within the system, but the requester is not notified of the procedures for making those corrections.

7.4 If no redress is provided, are alternatives are available?

Redress procedures are in place (see 7.2 above), and can be initiated through the FOIA/PA Office at USCIS.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals may request access to, or correction of, their personal information pursuant to the Freedom of Information Act and Privacy Act of 1974.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

The DHS Password Issuance and Control System (PICS) Office controls user authorizations and authentication controls for all DHS system users. Officers that have read-only access include adjudications officers who review applications and assign benefits as well as 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. Other external users who have solely read-only access include the Central Intelligence Agency, the Federal Bureau of Investigation, the Internal Revenue Service, Secret Service, the SSA and DOS. All users must access the system formally through terminal emulation software and TCP/IP access, as documented in the system's security documents. (see Section 4 at page 11 for details on information sharing). All users have cleared access to system resources granted through the DHS PICS Office.

CIS is a legacy INS mainframe system. Currently, ICE manages the contract for all legacy mainframe systems using the existing DOJ Data Center where CIS is located. This will change over time when DHS establishes its own data center that can house the mainframe systems. DOJ is responsible for the operation and maintenance of the mainframe and applications that run on the mainframe. There is a current Service Level Agreement (SLA) that defines DOJ responsibilities for intrusion detection, physical security, operational security, contingency controls, and reporting of security alerts and incidences. The SLA also defines levels of service to be provided. DHS is responsible for CIS application maintenance, development and testing. These services are performed through contractors. The USCIS ISSO works directly with the USCIS OIT, ICE IT, and DOJ to ensure that the SLA is current.

The Rules of Behavior for using the CIS application fall under the DHS guidelines for corporate rules of behavior. These rules are clarified and mandated to the user by the DHS guidelines and security documentation. The DHS PICS Office owns copies of these rules. Users agree to abide by these rules when receiving a secured User ID and upon passing a background clearance check.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractor personnel have access to CIS, perform maintenance software support to correct system problems, and service a Help Desk that provides support Monday through Friday for CIS-related issues.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the system allows users access to specific transactions. For example, users that are only authorized to read only access will only have access to the read and display transactions.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Both contractors and government personnel have access to CIS. Security procedures are in place in accordance with the system security plan and the USCIS systems lifecycle methodology. This plan is the primary reference that documents system security responsibilities, policies, controls, and procedures. Access to CIS is controlled via the DHS Password Issuance and Control System (PICS) Office controls user authorizations and authentication controls for all DHS system users. CIS is a mainframe system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Transactions are assigned by a USCIS Records Supervisor and reviewed regularly to ensure that users have appropriate access to CIS. Transactions are stored in the Password Issuance Control System.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

CIS is a legacy INS mainframe system that was under DOJ. Currently ICE manages the contract for all legacy mainframe systems using the existing DOJ Data Center where CIS is located. This will change over time when DHS establishes its own data center that can house the mainframe systems. DOJ is responsible for the operation and maintenance of the mainframe and applications that run

on the mainframe at the data center because they own the data center. There is a current Service Level Agreement (SLA) that defines DOJ responsibilities for intrusion detection, physical security, operational security, contingency controls, and reporting of security alerts and incidences. The SLA also defines levels of service to be provided. DHS is responsible for CIS application maintenance, development, and testing. These services are performed through contractors. The USCIS ISSO works directly with the USCIS OIT, ICE IT, and DOJ to ensure that the SLA is current.

The Rules of Behavior for using the CIS application fall under the DHS guidelines for corporate rules of behavior. These rules are clarified and mandated to the user by the DHS guidelines and security documentation. The DHS PICS Office maintains copies of these rules. Users agree to abide by these rules when receiving a secured User ID and upon passing a background clearance check.

Misuse of data in CIS is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and are adequately trained regarding the security of their systems.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All system users take annual mandatory Federal IT Security Awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data integrity, as well as the handling of data (including any special restrictions on data use and/or disclosure). The USCIS OIT IT Security office verifies that training has been successfully completed and maintains a record of certificates of training on all USCIS employees and contractors. Current CIS users took the mandatory USCIS IT security awareness training in May/June 2007.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

CIS secures the information by complying with the requirements of the DHS IT Security Program Handbook. CIS was granted an Unconditional Certification and Accreditation (C&A) on December 23, 2003. The C&A renewal process is currently underway, and is expected to be completed August 2007. CIS Sensitivity Level is 3, as determined in the Sensitive System Security Plan, because the unavailability of the data would have a significant impact on DHS functions.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: The primary risk is unauthorized access to or disclosure of information contained within CIS

Mitigation: To mitigate this risk, a number of business and systems rules have been implemented. Access to the database is given only to users that need it to perform their official duties. All authorized users must authenticate using a UserId and password.

Privacy Risk: Information security

Mitigation: USCIS has adopted the following information security practices to ensure information security:

USCIS offices are located in buildings with controlled access by security guards or authorized contractors for the government. Access to premises is by official identification. Information in this system is also safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards include restricting access to authorized personnel who have a need-to-know including the DHS Information Technology Security Programs Handbook using password protection identification features. CIS is maintained at the DOJ Data Center (Dallas). Physical controls of the facility (e.g., guards, locks, etc.) apply and prevent entry by unauthorized entities. The system does not contain classified information.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

CIS was custom-designed in 1985 to replace the old Master Index System to support legacy INS (now USCIS under DHS) records management needs to collect, store and disseminate automated biographic and historical information related to individuals of interest to DHS.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Throughout the investment's lifecycle, the integrated project team (IPT) security representatives have assessed the security requirements to comply with OMB and NIST regulations. The investment's Project Manager ensured that all security requirements were incorporated and tested before deployment of any new system features. Compliance with DHS and Federal policies,

procedures, guidelines, and standards were verified by the DHS Homeland Security Information Systems Security Program and external to DHS organizations through scheduled and unscheduled audits, reviews, and tests.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, USCIS designed the system to restrict government access to only those who have authority and the "need-to-know" access to specific data. System administrators based on this principle assign Userids and Passwords. All CIS data is transmitted, stored, and maintained in a secure data repository. Transactions are tracked in an audit log and stored for an indefinite period of time.

Responsible Officials

Contact Point: Elizabeth Gaffin
Privacy Officer, U.S. Citizenship and Immigration Services
(202) 272-1400

Reviewing Official: Hugo Teufel III
Chief Privacy Officer, Department of Homeland Security
(703) 235-0780

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security