Privacy Impact Assessment
for the

Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)

August 13, 2009

Contact Point
Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
202-272-1400

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

United States Citizenship and Immigration Services (USCIS) is developing the enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) to streamline access to relevant information by consolidating information collected during the adjudication of applications and petitions (hereafter referred to collectively as "applications") for immigration benefits. eCISCOR will serve as an intermediary repository for immigration and naturalization information derived from several USCIS systems and will replace the Citizenship and Immigration Services Centralized Oracle Repository (CISCOR). USCIS is conducting this Privacy Impact Assessment (PIA) because eCISCOR contains personally identifiable information (PII).

Overview

The USCIS Office of Information Technology (OIT) is developing eCISCOR to consolidate and manage immigration and naturalization information from several USCIS data systems thereby reducing the labor involved in accessing, reporting, and sharing information and expediting sharing initiatives between USCIS systems, Department of Homeland Security (DHS) components, and other agencies. eCISCOR will be designed as an intermediary database for current read-only application systems that require access to the immigration and naturalization data. As an intermediary database, eCISCOR will support workflow management, performance measurement, and information sharing requests from external users. Further, consolidating multiple data systems to one centralized repository makes it easier to secure, manage, monitor, and preserve the accuracy of immigration and naturalization data.

eCISCOR will serve as a repository for immigration and naturalization information and replace the existing composite system known as CISCOR. The CISCOR database consolidates data from USCIS's five Computer-Linked Application Information Management System 3.0 (CLAIMS 3) service center local area networks (LANs) to support CLAIMS 3 adjudications, workflow management, performance measurement, and ad hoc queries. After development, CISCOR experienced issues with its replication process, which limited its ability to adequately capture CLAIMS 3 LAN data changes in a timely manner. eCISCOR will be modeled after CISCOR but will utilize replication technology that will immediately capture data changes in the source system to prevent data discrepancies.

eCISCOR will be developed and implemented in an effort to streamline access to information by consolidating immigration and naturalization information from several USCIS systems into a centralized repository. eCISCOR will replicate and load read-only records from the following systems:

- **Computer-Linked Application Information Management System 3.0 (CLAIMS 3)** is a case management system used to process all immigration benefits except naturalization, asylum, and refugee status;
- **Computer-Linked Application Information Management System 4.0 (CLAIMS 4)** is an electronic case management application tracking and processing system used to process and adjudicate the Form N-400, *Application for Naturalization*;
- **Applications for Naturalization Central Index System (CIS)** is a system that supports a legacy Immigration and Naturalization Services records management need to collect and disseminate automated biographic and historical information on the status of applicants seeking immigration benefits;
- **Refugee, Asylum and Parole System (RAPS)** is a system that provides case management functionality for asylum and refugee cases;

- **Alien's Change of Address Form (AR-11)** tracks address changes that are submitted by individuals who use the Form AR-11;
- **National File Tracking System (NFTS)** is used to track alien file (A-File) location information;
- **Reengineered Naturalization Casework System (RNACS)** is used to process requests for the Form N-600, *Application for Certificate of Citizenship* and the Form N-565, *Application for Replacement Naturalization/Citizenship Document*;
- **Marriage Fraud Amendment System (MFAS)** is used to process requests for the Form I-751, *Petition to Remove Conditions on Residence* and the Form I-829, *Petition by Entrepreneur to Remove Conditions*; and
- **Enterprise Service Bus (ESB) Background Vetting Service (BVS)** is used to determine whether a specified offense against a minor is included in an individual's criminal history record originally derived from the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS).

The read-only replicated data will flow unidirectionally from the source system to eCISCOR.

The replication process will include extracting data from the source system and loading the extracted data into eCISCOR. Data will be replicated "as is." These data elements include, but are not limited to the applicant's name, alias, alien number (A-number), address, gender, marital status, date of birth, country of birth, country of nationality, ethnic origin, religion, Social Security Number (SSN), if available, personal characteristics, and criminal history record. Photographs will not be stored in eCISCOR. eCISCOR will include refresh enhancements to ensure the completeness of data within eCISCOR. This will allow USCIS to preserve the integrity and accuracy of the information derived from USCIS systems.

eCISCOR will be responsible for replacing and supplementing the reporting and sharing capability of the source system. The USCIS systems that facilitate such functions are constructed from a conglomerate of technologies causing USCIS personnel to perform a complex set of queries against each system to access data needed to analyze the business operations and share data as needed. eCISCOR will interface with the following applications:

- **Standard Management Analysis Reporting Tool (SMART) –** to facilitate USCIS's ability to measure the production metrics. SMART users are limited to USCIS employees.
- **Person Centric Query System (PCQS)** - to support sharing initiative between the DHS, USCIS, and Department of State (DOS), Bureau of Counselor Affairs to share immigration and visa data between agencies as documented in the PIA for the USCIS Person Centric Query System published on June 22, 2007. PCQS users are limited to USCIS, DHS, and DOS employees.
- **ESB BVS –** to assist USCIS's ability to determine if a petitioner is eligible to receive an immigration benefit as documented in the PIA for the USCIS Background Vetting Service. ESB BVS users are limited to USCIS employees.

User access and data presentation will be controlled by these individual applications. eCISCOR will provide these applications with greater accessibility to immigration and naturalization information required for these initiatives, while reducing resources currently used to access these systems individually.

eCISCOR is a growing and expanding project. As eCISCOR matures, and future enhancements and components are developed, this PIA will be revised to address those updates.

The legal authority for eCISCOR is derived from 8 U.S.C. §1101 *et seq*.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

eCISCOR will replicate the following source system data elements in order to consolidate the data and streamline the process for reporting and information sharing initiatives:

- **Names:** first, middle or initial, family, aliases, maiden, current/prior spouse's, children's, person who prepared the form;
- **Addresses:** home, current and prior spouse's, children's, applicant's e-mail, person who prepared the form, applicant's/spouse's employer;
- **Telephone Numbers:** applicant's or form preparer's telephone number;
- **Birth Information:** applicant, spouse, and children birth dates, and country of birth;
- **Social Security Numbers (SSNs):** SSNs for some applicants and some current spouses; the SSN fields will not be automatically exposed to eCISCOR users unless there is a business need that requires access of the SSN field;
- **Citizenship/Nationality Information:** applicant's race/country of nationality, spouse, date current spouse obtained citizenship, place spouse became a citizen;
- **Information Regarding Immigration Status:** applicant, current/prior spouse's A-Number and dates the applicant entered into and exited from the U.S. (days spent outside the U.S., trips outside the U.S.);
- **Marital Status/Family Information:** current and prior marriages or prior separations, prior spouses, date of marriage/divorce, number of marriages for applicant and spouse, reason prior marriage ended, whether applicant has ever been married to multiple persons at the same time, and family information (number of children);
- **Personal Characteristics:** hair color, eye color, height, gender, weight, languages spoken;
- **Tax Payment and Financial Information:** failure to pay taxes; owed taxes; claimed non resident status for tax purposes; failure to file taxes because of nonresident status; applicant/spouse's earnings per week; amount in bank accounts; value of vehicles, real estate, and others assets; parents' estimated assets/weekly earnings;
- **Employment Information:** place and address of employment/occupation, type of work, employer name, length of employment, spouse's employment;
- **Case management records**: NFTS file location result;

- **Criminal history record (RAP Sheet)**: RAP sheet text, FBI Number, US-VISIT Encounter ID, US-VISIT Enumerator, True/False indicator stating whether or not RAP Sheet text contains crimes against minor.

- **Military and Selective Service Information:** information evidencing Selective Service registration and military service (e.g., Selective Service number, date of registration, application for military exemption, military branch, willingness to bear arms for the U.S.).

1.2 What are the sources of the information in the system?

eCISCOR will collect and maintain immigration and naturalization information replicated from the following systems: CLAIMS 3, CLAIMS 4, CIS, RAPS, AR-11, NFTS, ESB BVS, RNACS, and MAFS. The source for most of the information in these systems is the completed immigration application, which is submitted by applicant seeking benefit and validated by applicant when interviewed.

Additional data sources will follow in future releases. eCISCOR may have access to and collect data from other USCIS application systems and legacy systems.

1.3 Why is the information being collected, used, disseminated, or maintained?

eCISCOR will provide a consolidated view of immigration and naturalization information, optimized for USCIS related reporting and information sharing purposes. eCISCOR will be a intermediary repository that maintains immigration and naturalization information from several USCIS systems. This system will act as the source database for SMART, ESB BVS, and PCQS. Consolidating multiple data systems to one centralized repository will minimize the resources spent on accessing these systems individually.

eCISCOR may also retain a collection of all legacy USCIS system data, in accordance with its respective retention schedule, for historical need as legacy systems are decommissioned.

1.4 How is the information collected?

eCISCOR will not collect information directly from the individual. Information maintained in eCISCOR will be collected only from the source system. Most of the information in the source system will be collected directly from the individual about whom the information is collected. This information will then be transferred to and stored in eCISCOR. Data transmission will be designed and implemented using secure communication mechanisms as required in DHS security protocols.

eCISCOR will eventually interact with several other USCIS systems through secure communication mechanisms as required by DHS security protocols and collect replicated data from those source databases.

1.5 How will the information be checked for accuracy?

eCISCOR will be dependent on the accuracy and quality of information provided by the source system. eCISCOR will ensure the accuracy of the data by collecting the information directly from the source system, which typically collects its data directly from the individual about whom the information is

collected. eCISCOR will also receive updates from the source system on a daily basis. This updated information will include any changes made to the data by the individual applicant as they proceed through the adjudication process. Please see the source system PIA (available at www.dhs.gov/privacy) for a detailed discussion of the numerous opportunities individuals have to correct their personal information during the immigration and naturalization process.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authority for eCISCOR comes from 8 U.S.C. § 1101 *et seq*. (Alien and Nationality Act).

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

Privacy Risk: Unauthorized access to or disclosure of information contained within eCISCOR.

Mitigation: Access to eCISCOR will be given only to a limited number of government and contractor users for the purpose of developing eCISCOR. Users will have administrator privileges and duties in order to ensure that eCISCOR properly captures data changes from the source system. All authorized users will have to authenticate using a user ID and password. Otherwise, users may access data maintained in eCISCOR via the SMART, ESB BVS, and PCQS applications. Lastly, through policies and procedures, DHS will limit the use and access of all data in eCISCOR to the purposes for which it was originally collected as described in the source system Privacy Act system of records notice (SORN).

Privacy Risk: Data inaccuracies

Mitigation: eCISCOR will be dependent on the accuracy and quality of information provided by source system. eCISCOR will be developed to include refresh enhancements to ensure the completeness of data within eCISCOR. The refresh technology will identify and capture the data that were changed within source system. In order to efficiently capture data changes, data derived from the sources system will be updated at least on a daily basis. This process will reduce the risk of data discrepancies between eCISCOR and the source system. In addition, eCISCOR access will be limited to read-only connectivity, thus preserving the integrity and accuracy of the information derived from USCIS systems.

Privacy Risk: Collection of extraneous information

Mitigation: eCISCOR will collect a minimum set of PII from the source system (as described in Section 1.1). The eCISCOR database will contain only those data elements needed to accomplish the searches required for reporting and information sharing purposes. As eCISCOR evolves, the database will collect a minimum set of PII derived from other USCIS systems.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

eCISCOR will consolidate data from several USCIS application systems. This repository will centralize information and act as the source database for SMART, ESB BVS, PCQS. These applications will access eCISCOR for reporting and information sharing purposes.

2.2 What types of tools are used to analyze data and what type of data may be produced?

eCISCOR will not have data analysis capabilities. eCISCOR will not be used to perform complex analytical tasks resulting in data matching such as relational analysis, scoring, reporting, or pattern analysis. Data will not be changed during replication other than to provide a consolidated snapshot of the data. Moreover, the system will not create or make available new or previously unavailable data from newly derived information.

In the future, USCIS management may choose to implement some analytical functions. This PIA will be updated if that occurs.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The source systems do not collect, use, or maintain commercial or publicly available data; therefore, eCISCOR will not maintain commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Inappropriate use of the information

Mitigation: User access to eCISCOR data will be limited to those who need the information to perform their job functions. The system administrator will be responsible for granting the appropriate level of access. The SMART, ESB BVS, and PCQS users will indirectly access eCISCOR for reporting and information sharing purposes. All USCIS employees will be properly trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

DHS Management Directive System (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004, will provide guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information in both paper and electronic records (including eCISCOR). Additionally, all DHS employees will be required to take

annual privacy awareness and computer security training, which addresses this issue. DHS will also maintain rules of behavior for employees who use DHS systems.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

eCISCOR will collect data from CLAIMS 3, CLAIMS 4, CIS, RAPS, AR-11, NFTS, ESB BVS, RNACS, and MAFS. As the system develops in later stages, information from existing USCIS systems and legacy systems will be added. Data derived from all existing USCIS systems will be retained in accordance with data retention schedules specific to those systems.

eCISCOR will eventually retain a collection of all legacy USCIS system data as a read-only copy for historical need as legacy systems are decommissioned. As each source system is retired, a retention schedule for that final data set will be established.

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

eCISCOR will collect data from existing USCIS systems and legacy systems. Data derived from other systems will be retained in accordance with data retention schedules specific to those systems.

eCISCOR will eventually retain a collection of all legacy USCIS system data as a read-only copy for historical need as legacy systems are decommissioned. As each source system is retired, a retention schedule for that final data set will be established.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Maintaining personal information for a period longer than necessary to achieve agency objectives.

Mitigation: Although there is always risk inherent in retaining personal data for any length of time, the eCISCOR will replicate data from systems whose data retention periods identified in the NARA schedule are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. The schedules proposed and approved by NARA for each source system match the requirements of the Federal Records Act and the stated purpose and mission of the system. The time periods in the source systems' NARA schedules were carefully negotiated between USCIS and NARA to ensure that data is retained for the minimum time needed to process the application and make the information available for other USCIS benefits that might be sought by an applicant.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

PCQS will query data from eCISCOR. The DHS users of PCQS are users within USCIS, Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP). Users of the PCQ Service within USCIS are those with adjudication responsibilities. Users of the PCQ Service within ICE are those with immigration investigation purposes. Users of the PCQ Service within CBP are those with border enforcement purposes.

4.2 How is the information transmitted or disclosed?

All internal sharing will be conducted over a secure and reliable DHS electronic interface or secure courier. This interface utilizes secure network connections on the DHS core network. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, and M-06-16 *Protection of Sensitive Agency Information*, dated June 23, 2006, setting forth the standards for the handling and safeguarding of personally identifying information.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: Unauthorized access to eCISCOR PII (including searches beyond the scope of the user's duties) both during transmission and after it is shared.

Mitigation: The PCQS is only available to authorized users who have been granted the appropriate privileges to access data and who need the information to perform their job functions. All authorized PCQS users must authenticate using a user ID and password. DHS policies and procedures are also in place to limit the use of and access to all data in eCISCOR to the purposes for which it was collected. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. An audit trail will be kept for system access and all transactions that request, create, update, or delete information from the system. The audit log, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access, or destruction.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The PCQ Service will query data from eCISCOR. The DHS external users of this data are users within the DOS Bureau of Consular Affairs. Users of the PCQ Service within the DOS's Bureau of Consular Affairs are those with VISA and Passport adjudication responsibilities, as well as those with Fraud Detection and investigation responsibilities. External sharing will be consistent with existing routine uses covered by the applicable source system SORN.

Future releases of eCISCOR may open up communication interfaces with other, yet to be developed, applications that may share information with external organizations. External sharing will be covered by the routine uses covered by the applicable SORNs. This PIA will be updated accordingly if eCISCOR shares information to other external organizations

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

A Memorandum of Understanding (MOU) exists between DHS and DOS that fully covers the eCISCOR and PCQS interface. The MOU clarifies the authority for DOS and DHS to share immigration and naturalization records and the basic mechanisms established to protect this data. Further, the sharing of information is compatible with the routine uses outlined in the SORN for each source system.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information in eCISCOR is tightly controlled and access via PCQS is granted only to individuals (internally and externally) with a specific need to access the system in order to perform their duties. Each transmission of data from eCISCOR to an internal or external system is covered by an Interface Control Agreement (ICA) that describes the electronic system interface, the levels of authentication, access control that are needed, and the data to be shared. The ICA also describes the security controls that protect the interface.

External entities will not have uncontrolled access to the eCISCOR (e.g., external entities have read only access). Once the data is shared, however, the receiving agency is responsible for safeguarding and assuring proper use of the data within its organization. Each of these sharing arrangements is covered by an

appropriate routine use in the source system SORN.

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

Privacy Risk: The primary privacy risk in external sharing is the sharing of data for purposes that are not in accord with the stated purpose and use of the original collection.

Mitigation The information collected and maintained by eCISCOR will be shared with organizations internal or external to DHS in accordance with the source system SORNs. If future modifications to the eCISCOR system call for additional external sharing, all external eCISCOR sharing arrangements will be consistent with existing routine uses or performed with the consent of the individual whose information is being shared, unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements. These routine uses limit the sharing of information from the system to the stated purpose of the original collection.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

eCISCOR will replicate and store data from several USCIS systems. eCISCOR will be covered by the SORN for each system that it collects. eCISCOR is covered by the following SORNS:

DHS/USCIS Alien File (A-File) and Central Index System (CIS) System of Records last published on January 16, 2007 (72 FR 1755) covers CIS and NTFS;

DHS/USCIS Benefit Information System (BIS) System of Records last published on September 29, 2008 (73 FR 56596) covers CLAIMS 3, CLAIMS 4, RNACS, AR-11, and MFAS;

DHS-USCIS Background Check System (BCS) System of Records last published on June 5, 2007 (72 FR 31082); and

FBI Integrated Automated Fingerprint Identification System (IAFIS) System of Records last published on September 28, 1999 (64 FR 52343) covers ESB BVS.

Additionally, the primary source of information for USICS systems is the application filed by the applicant or on their behalf by a sponsoring individual or organization. USCIS applications contain a Privacy Act statement and a provision by which an applicant authorizes USCIS to release any information received from the applicants as needed to determine their eligibility for immigration and naturalization benefits.

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

The data collected from the source system by eCISCOR will be a consolidated view of an individual's immigration and naturalization status. This information is provided by the applicant through the application for USCIS benefit. Individuals who submit applications for USCIS immigration benefits are asked to provide their consent to enable USCIS to release information provided to USCIS, to assist in the determination of an individual's eligibility for the benefit being sought. Specifically, the application includes a Privacy Act Notice and requires the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." The individual has the right to decline to provide the required information and consent. However, the failure to do so may result in the denial of the requested benefit request.

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

eCISCOR does not collect information directly from the individual; rather, it replicates information from the source system. This information is provided by the applicant through the application. The application requires that applicants must complete all data fields in the form. This information is critical in making an informed decision regarding USCIS benefits. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application and thus precludes the applicant from obtaining naturalization. Therefore, the individual has the right to decline to provide the required information and consent, but the failure to do so may result in the denial of the requested benefit request.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Applicants are unaware of the purposes for which their information is used.

Mitigation: Applicants applying for immigration benefits will be made aware that the information they are providing is being collected to determine whether they are eligible for their respective benefit. The USCIS application contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants will also be advised that the information provided will be shared with other Federal, state, local and foreign law enforcement and regulatory agencies during the course of the investigation. In the USCIS Privacy Notice,[1] individuals will also be notified that electronically submitted information is maintained and destroyed according to the requirements of the Federal Records Act NARA regulations and records schedules, and in some cases may be covered by the Privacy Act and subject to disclosure under the Freedom of Information Act (FOIA). OMB approved all Privacy Act Statements on USCIS forms used to collect data.

[1] Available at http://www.uscis.gov/portal/site/uscis/privacy_policy.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Any individual seeking to access information maintained in eCISCOR 1.0 should direct his or her request to the USCIS FOIA / Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403-6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010 (all other USCIS records). The process for requesting records can be found at 6 Code of Federal Regulations, Section 5.21. Requests for records amendments may also be submitted to the service center where the application was originally submitted. The request should state clearly the information that is being contested, the reasons for contesting it, and the proposed amendment to the information. If USCIS intends to use information that is not contained in the application or supporting documentation (e.g., criminal history received from law enforcement), it will provide formal notice to the applicant and provide them an opportunity to refute the information prior to rendering a final decision regarding the application. This provides yet another mechanism for erroneous information to be corrected.

As eCISCOR evolves, it will consolidate data from multiple USCIS application systems. Individuals may request access to their information by submitting a Privacy Act request unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements.

7.2 What are the procedures for correcting inaccurate or erroneous information?

eCISCOR will not maintain any mechanisms that allow individuals to amend erroneous information. However, the source systems maintain procedures that allow individuals to gain access to their information through redress procedures as described in the applicable SORN (See Section 6.1 for more details). eCISCOR will maintain read-only data obtained from the data source and no procedures will be in place that allows USCIS personnel to amend eCISCOR records. eCISCOR will have a refresh mechanism that automatically updates the source systems records; thus, ensuring timely and accurate data.

The source system will be fully responsible for the data replicated by eCISCOR. Requests to contest or amend information contained in source system should be submitted as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access. Moreover, when an applicant is interviewed by a USCIS adjudicator, the applicant also has the opportunity to make changes to his or her information in the source system.

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

eCISCOR will not employ mechanisms or procedures to notify individuals on how to amend their information. The SORNs and PIAs for the source systems will provide individuals with guidance regarding the procedures for correcting erroneous information (See Section 6.1 for a full discussion).

7.4 If no formal redress is provided, what alternatives are available to the individual?

If eCISCOR is maintaining erroneous data, it will be the responsibility of the source data system owner to ensure that the data is corrected. Individuals will be provided opportunity for redress as discussed above in section 7.1.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: The main risk with respect to redress will be that the right may be limited by the deployment of Privacy Act exemptions or limited avenues for seeking redress and amendment of records.

Mitigation: The redress and access measures offered by USCIS will be appropriate given the purpose of the system. Individuals will be given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources. USCIS allows individuals to request access to amend their information by submitting a Privacy Act request unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

Direct access will be limited to authorized USCIS employees and contractors. In compliance with federal law and regulations, users will have access to eCISCOR on a need to know basis. This need to know will be determined by the individual's current job functions. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. SMART, ESB BVS PCQS users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements.

8.2 Will Department contractors have access to the system?

Contractors maintain eCISCOR under the direction of USCIS OIT. Access will be provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant SOPs. In addition, USCIS employees and contractors who have completed the system access application process and been granted appropriate access levels by a supervisor will be assigned a login ID and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation to obtain the appropriate access levels.

eCISCOR will offer the following six levels of access:

Class 1 – O&M System Administration - Users requiring System Administration privileges to backup or maintain the system.

Class 2 – O&M Database Administration - Users requiring minimal Database Administration privileges to backup or maintain the system.

Class 3 – Database Developer - Users requiring full Database Administration privileges to design, develop, and optimize the system.

Class 4 – Application Developer - Users requiring developer level privileges to a specific schema on the development server to design, develop, and optimize server side objects for application interfaces.

Class 5 – Data Miner - Users requiring search capabilities.

Class 6 – Application Account - Applications requiring read only search capabilities on the eCISCOR database.

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

All federal employees and contractors will be required to complete annual privacy awareness and computer security awareness training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. eCISCOR received a Full Certification and Accreditation (C&A) on September 16, 2008 (expiration is September 16, 2011).

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

In accordance with DHS security guidelines, eCISCOR will use auditing capabilities that log user activity. All user actions will be tracked via audit logs to identify audit information by user identification,

network terminal identification, date, time, and data accessed. eCISCOR will employ auditing measures and technical safeguards to prevent the misuse of data. Many users have legitimate job duties that require them to design, develop, and optimize the system. This work will be performed under supervisory oversight. Furthermore, each employee will be given annual security awareness training that addresses their duties and responsibilities to protect the data.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Unauthorized access to personal information.

Mitigation: Access and security controls will be established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Role-based user accounts will be used to minimize the number of persons who have access to the system. Audit trails will be kept in order to track and identify any unauthorized changes to information in the system. eCISCOR will have a comprehensive audit trail tracking and maintenance function that records the activity of the user. All personnel will be required to complete annual online computer security training.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

eCISCOR 1.0 will be an enterprise data warehouse.

9.2 What stage of development is the system in and what project development lifecycle was used?

eCISCOR 1.0 is in the development testing phase of the DHS Development System Life Cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

eCISCOR will not employ technologies that may raise privacy concerns. eCISCOR will contain only the information collected during the administration and adjudication of applications in the source system for reporting and information sharing purposes. eCISCOR will not have any ability to track, or in any way monitor, the activities or applications of individuals outside of the information required to process the applications.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security