Privacy Impact Assessment
for the

USCIS
Secure Information Management Service (SIMS) Pilot with Inter-country Adoptions

May 24, 2007

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

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

Abstract

United States Citizenship and Immigration Services (USCIS) prepared a Privacy Impact Assessment (PIA) for the Secure Information Management Service (SIMS) Pilot. Using the inter-country adoption caseload as a "proof-of-concept" for SIMS, this pilot will: (a) demonstrate the case processing capability of the case management system, (b) verify that an enumerator (unique identifier based on biometrics) supports the USCIS person-centric business process, and (c) verify that the case management system can be used to view digitized files. This PIA covers the initial deployment of the SIMS and will be supplemented accordingly as additional USCIS applications and system functionalities are added to the SIMS.

Introduction

The Department of Homeland Security (DHS) through United States Citizenship and Immigration Services (USCIS) implements United States (U.S.) immigration law and policy through the processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. USCIS also supports national security by preventing individuals from fraudulently obtaining immigration benefits and by denying applications from individuals who pose national security or public safety threats to the U.S.

USCIS is embarking on an enterprise-wide "Transformation Program" that will transition the agency from a fragmented, form-centric, and paper-based operational environment to a centralized, person-centric, consolidated environment utilizing electronic adjudication. A person centric environment is USCIS' proposed method for doing business with customers, because it will enable the agency to focus more on the individual rather than the type of form they submit. The new operational environment will employ the types of online customer accounts used in the private sector. This person-centric model will link information related to an individual in a single account in order to facilitate customer friendly transactions, track activities, and reduce identity fraud.

To support this effort, USCIS is deploying a series of pilots to validate key concepts of the program's mission. One of the key functions of the SIMS Pilot deployment is to demonstrate the overall benefits of the USCIS Transformation Project. Using the inter-country adoption caseload as a "proof-of-concept" of the SIMS, this pilot will demonstrate the case processing capability of the case management system, verify that an enumerator (unique identifier based on biometrics) supports the USCIS person-centric business process, and verify that the case management system can be used to view digitized files.

What is SIMS?

The SIMS is a web-based, information and case management service that enables USCIS to perform end-to-end processing of applications and the ability to better associate and manage relationships with its applicants.

The SIMS Pilot will utilize the Enumeration Services[1] of DHS's US-VISIT Program, when deployed, to establish a unique identity for each individual interacting with USCIS. Enumeration Services will establish an enterprise-wide unique personal identifier, known as the enumerator, based on 10 fingerprints and limited biographic information of an individual. An enumerator is a randomly generated alphanumeric unique identifier that is used to link disparate records associated with an individual for the purpose of identification. Enumeration will allow USCIS to consolidate information on an individual and facilitate identity verification, risk evaluation, and benefit eligibility.

It is important to note that the SIMS Pilot can deploy if the Enumeration Services of US-VISIT are not available at time of the SIMS Pilot deployment. Although the enumerator provides a significant benefit to USCIS in establishing the unique identify of an individual, it is not required of USCIS to perform the adjudication of an adoption case.

In addition, the SIMS Pilot will utilize digitized A-Files generated through USCIS' Integrated Digitization Document Management Program (IDDMP)[2]. IDDMP will enable USCIS to scan, store, and view immigration paper files and related documents while integrating to person-centric records, making them electronically available to USCIS and other agencies.

Why Inter-Country Adoption?

The inter-country adoption (herein referred to solely as 'adoption') caseload was identified by USCIS leadership as an ideal target area for the initial deployment of the SIMS Pilot for multiple reasons:

1. Adoption is a low-volume caseload (USCIS processes approximately 20,000 – 30,000 applications per year).
2. Adoption cases are processed by a limited number of adjudicators (approximately 100 adjudicators handle adoption cases).

[1] For privacy information related to Enumeration Services, refer to the US-VISIT PIA created for Enumeration Services.

[2] For privacy information related to Integrated Digitization Document Management Program (DDMP), refer to the USCIS PIA created for the IDDMP that can be found at: http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#4

3. Adoption is not currently supported by any USCIS-wide information technology (IT) solution; therefore implementing a case management solution does not require data migration or the decommissioning of a legacy system.
4. The centralization of domestic operations can be leveraged to support the intake of customer supplied information and to better assist USCIS in the management of its workload.

Current Adoption Process

USCIS processes adoption cases under the authority of the Immigration and Nationality Act, 8 U.S.C. Section 1101(b) (1) (F). The current adoption process is a form-centric approach that focuses on a series of forms and independent processes, rather than a consolidated set of transactions focusing on the customer's primary request. Currently, a customer must file multiple applications to, 1) obtain parent qualification and approval, 2) adopt a child, and 3) obtain citizenship for a child.

Generally, customers residing in the U.S. must file adoption applications with the local USCIS office with jurisdiction over their place of residence in the U.S. Customers residing outside of the U.S. must contact the nearest American consulate or embassy that will take action on their application. Should a customer move during the adoption process, USCIS must transfer his case to a different jurisdiction, resulting in longer processing times and limiting access to the file to a single adjudicator. Utilizing paper-based files results in high transmittal costs and requires a complex record management system.

Customers may be engaged in the adoption process over a multi-year period depending upon the country from which they seek to adopt because of the differences in legal requirements in each foreign country. USCIS regulations dictate that applications (and associated home studies) expire in 18 months in order to ensure that information is current. As a result, customers may be required to re-file their applications and submit new home studies. Currently, re-filing is the same as starting the process all over again. This process results in additional cost and time to complete the filing requirements.

New Operational Concept

The new operational concept will facilitate interactions between USCIS and adoptive parents or their representatives. Each adoption application request would link to an existing SIMS account or trigger the creation of a new SIMS account that contains personally identifiable information. All adoption requests related to an individual will be contained in a SIMS case that tracks the actions required to adjudicate the adoption or naturalization request. The priorities of the new concept are as follows:

- Establish a person-centric view for individuals associated with a case, utilizing the Enumeration Service of the US-VISIT program to establish a unique identity for each individual that is required by USCIS to be fingerprinted.
- Provide a centralized, web-based repository for the data that provides access to all the documents related to a case, thereby eliminating the need for a paper case or a case file.

There are three key process areas (outlined below) supporting the new operational concept. The components of the SIMS Pilot support this concept as well as the overall objectives of the USCIS Transformation Program.

1. **Intake:** Registration and Application Submission – For purposes of the pilot, applications will be submitted via mail. USCIS personnel will manually create customer accounts for each applicant. The customer account number will be provided to the individual who can than use it as a reference number for all subsequent activities supporting the adoption or citizenship process. Each individual or organization involved in an adoption case will get a separate and unique account number. Only those individuals involved in an adoption case who are required by USCIS to be fingerprinted will receive an enumerator.
2. **Case Management:** Case Creation, Centralized Workload, and Workflow Management – Case Management entails electronically capturing, storing, and processing account and case data in a centralized environment allowing a limited number of authorized users to share data across USCIS while providing users with workflow tools to manage adoption cases effectively.
3. **Electronic Adjudication (by USCIS personnel):** Approval of Parents, Approval of Child, Verification of Visa Issuance, and Derivation or Acquisition of Citizenship – The electronic adjudication process follows a logical process which supports a consistent application of policies and business rules to address the major adjudication decision points for adoption.

Figure 1 below, provides an overview of the new operational concept, illustrating the steps of the adoption process that occur within each of the three process areas.

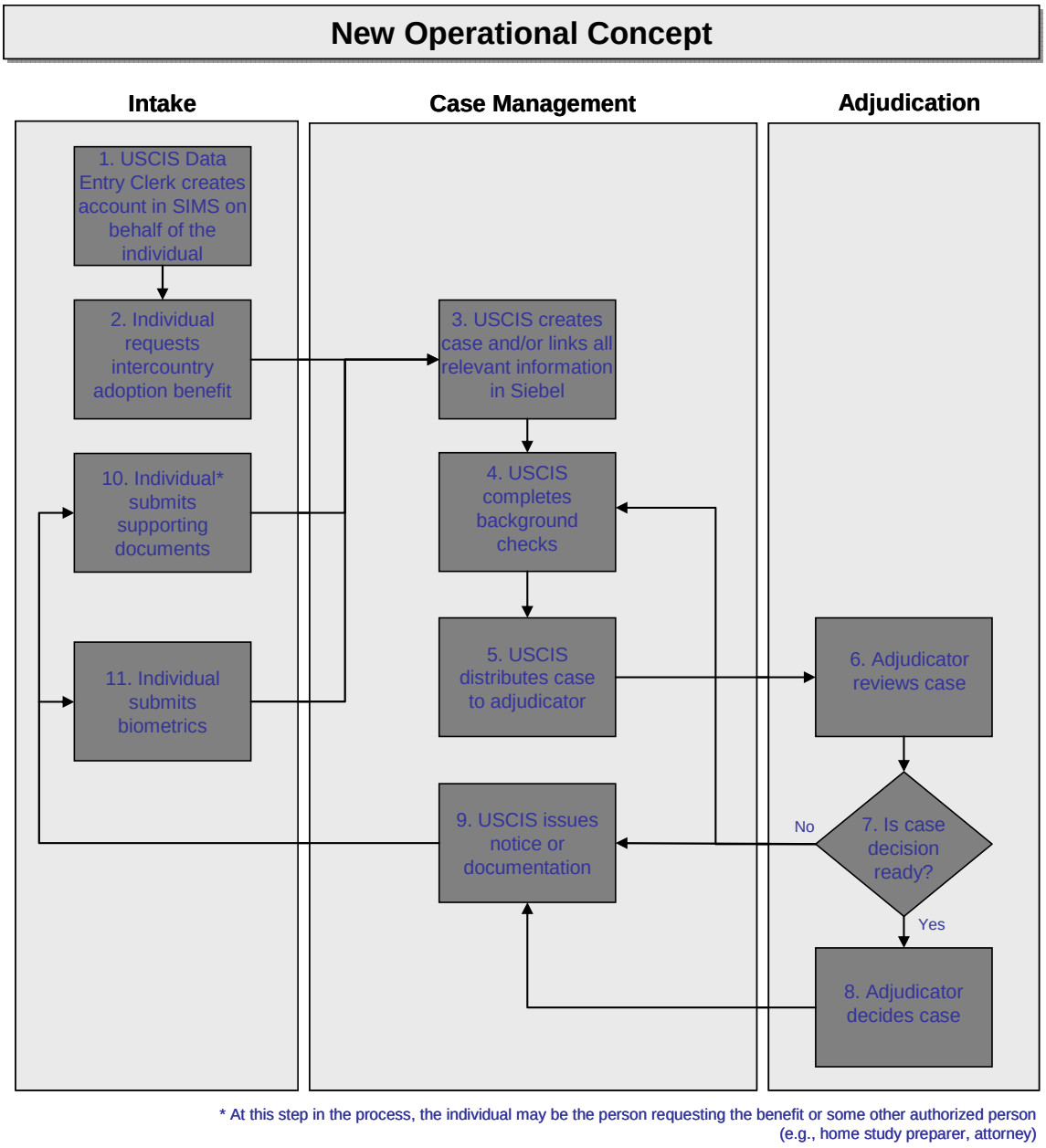

Figure 1 – New Operational Concept Diagram

Each of the steps occurring within the key process areas (e.g. Intake, Case Management and Adjudication) represents a core function of the new operational concept. *Appendix A* provides a description of these steps in relation to both the pilot process and the proposed, long-term vision of the SIMS.

Pilot Scope

For purposes of the SIMS Pilot, the following items are considered within scope to meet the needs of the new operational concept:

- The SIMS Pilot will be implemented to process newly received cases on a date-forward basis.
- The SIMS Pilot will consist of approximately 100 initial USCIS users (this includes adjudicators, supervisors, data entry staff, Application Support Center (ASC) staff and customer support representatives).
- For adoption cases processed overseas, the SIMS Pilot will incorporate a limited number of users at international sites specified by USCIS.
- The SIMS Pilot will not impact existing paper-based processes.
- For purposes of the SIMS Pilot, internal USCIS data entry staff will create customer accounts when paper applications are submitted.
- The SIMS Pilot will utilize the Enumeration Services of the US-VISIT program to assign an enumerator that links biometric and biographic data in the SIMS.
- The SIMS Pilot will utilize digitized files generated through USCIS' IDDMP.

As part of the SIMS Pilot, DHS is updating and re-issuing the legacy System of Records Notice, Department of Justice DOJ/Immigration and Naturalization (INS) – 007 SORN known as Orphan Petitioner Index and Files that was published on July 27, 2001, 66 FR 39199. As part of DHS's ongoing efforts to increase transparency and update legacy system of records notice, The legacy SORN will be retired and replaced with the DHS/USCIS – 005 Inter-country Adoptions system of records.

This PIA covers DHS's use of the SIMS Pilot and the information contained therein related to Inter-country Adoptions. This PIA will be updated as changes are made to the adoptions process and its use of SIMS.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The SIMS collects and stores information on individuals and organizations associated with the following:

- Filing of the Office and Management and Budget (OMB)-approved versions of USCIS adoption related forms/applications;
  - Form I-600, *Petition to Classify Orphan as an Immediate Relative*
  - Form I-600A, *Application for Advance Processing of Orphan Petition*

- Form N-600, *Application for Certificate of Citizenship*
- Form N-600K, *Application for Citizenship and Issuance of Certificate under Section 322*

- Account setup data.

The information collected about these individuals and organizations includes, but is not limited to: name, addresses, phone numbers, family member names, citizenship status, marital status, social security numbers, dates of birth, places of birth, gender, height, biometrics, and results of background investigations (inclusive of home study checks, FBI checks, and name checks). Information will be collected from prospective parents as well as from other adults who may be residing in the household pursuant to 8 C.F.R. Section 204.3. In addition, limited information related to the biological parents of the child being considered for adoption may be collected in this system of records. Given the sensitivity surrounding the collection of social security numbers, USCIS collects this information solely on the OMB-approved version of the N-600 - *Application for Certificate of Citizenship*. The social security number is not a required field in the SIMS, and if an individual chooses not to provide this information to USCIS, it will not adversely affect the individual's benefit eligibility or the adjudicative decision on their case.

1.2 From whom is information collected?

The Inter-country Adoption implementation of SIMS collects and stores information on individuals and organizations associated with the filing of forms/applications on cases related to adoption. For the purpose of the Inter-country Adoption implementation of SIMS Pilot, an *individual* is defined as any person involved in an adoption case, including, but not limited to adoptive parents, children, other adults in the household, and organization members. An adult member of the prospective adoptive patent's household is defined as "an individual other than a prospective adoptive parent, over the age of 18 whose principal or only residence is the home of the prospective adoptive parents." An *organization* member is defined as any individual associated with any group or entity involved in an adoption case, including, but not limited to law firms, adoption home study providers, adoption placement agencies, and adoption non-profit organizations.

1.3 Why is the information being collected?

USCIS uses the information collected for the purposes of the Inter-country Adoption implementation of SIMS to make an adjudicative decision for each submitted application for adoption.

USCIS Domestic Field Offices, International District Offices and sub-offices collect the information to support end-to-end processing and adjudication of adoption applications, such as requests for obtaining orphan status for a foreign-born child and citizenship for an adopted child. Field Offices receive and validate documentation, conduct biometric and background checks, and determine applicant eligibility.

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

The Immigration and Nationality Act, 8 U.S.C. Section 1101(b) (1) (F) and 8 C.F.R. Section 204.3

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.

The primary risk of the Inter-country Adoption implementation of SIMS Pilot is unauthorized access to or disclosure of information contained within SIMS. To mitigate this risk, a number of business and system rules have been implemented. Access to SIMS is given only to a limited number of government and contractor users who need it to perform their official duties. All authorized users must authenticate using a user ID and password. Lastly, through policies and procedures, DHS limits the use and access of all data in SIMS to the purposes for which it was collected.

The Inter-country Adoption implementation of SIMS Pilot provides users with the ability to perform full queries on individuals and data stored within SIMS. With this function, there is a risk that users will search for information on individuals and topics beyond the scope of their work. This risk is mitigated by SIMS training and the enforcement of DHS policies that limit the use and access of all data in SIMS to the purposes for which it was collected. An audit trail will be kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access, or destruction, and kept for at least 90 days.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

USCIS uses the information collected by Inter-country Adoption implementation of SIMS internally to make an adjudicative decision for each submitted application for adoption. For purposes of the Inter-country Adoption implementation of SIMS Pilot, USCIS data entry personnel utilize the collected data to manually create customer accounts for each submitted application.

Additionally, the information collected by SIMS is used to:

- To generate Certificates of Citizenship
- To obtain Visas from the Department of State (DoS)

- Perform background checks and investigations (inclusive of home study checks, FBI fingerprint checks and name checks.)
- Facilitate cross-agency communication for fraud detection and law enforcement purposes

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No, SIMS is not currently designed, or used, to assist users in identifying previously unknown areas of note, concern, or pattern. In the future, internal DHS users may use the system to retrieve and view archived application data (e.g., previously submitted applications or home study reports) but data analysis is not a function of SIMS. If a new analytical tool is ever introduced to perform data analysis, a supplemental PIA will be created for that tool.

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

Although SIMS provides some automated alert functionality to the USCIS user, the onus falls on USCIS personnel to review the information collected during the formal adjudication process. USCIS uses a combination of supporting documentation (e.g., birth certificate, passport, etc.), background checks (e.g., fingerprint and name checks), and in-person interviews as appropriate to verify information collected from individuals.

In addition, current USCIS regulations dictate that home studies expire after 18 months in order to ensure that information on the adopting household is current. As a result, USCIS requires that a new and updated home study be submitted after the 18 month expiration period. USCIS will not make an adjudicative decision on the adoption case until a valid home study is provided.

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.

To ensure the information collected is being used for its intended purpose, a detailed user role matrix has been included as part of the SIMS requirements. This matrix provides an overall view of each role (user type) and their ability to create, read, update or delete (CRUD) information in the SIMS. The CRUD Matrix also depicts the hierarchical structure or "approval chain" that exists in each office processing adoption cases.

Currently, the SIMS maintains five user roles: 1) Customer Service Representative, 2) Data Entry Clerk, 3) Officer, 4) Manager, and 5) System Administrator. User roles are assigned to USCIS personnel and contractors based on the level of access the user needs to perform their work. All users must be authenticated by a userid and password prior to accessing the SIMS.

In addition, all USCIS personnel and contractors with access to SIMS are required to attend training on SIMS, which provides the users with an understanding of the appropriate and inappropriate uses of the information and the system.

Section 3.0 Retention

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

Records related to an individual (currently referred to as 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. C-File records are to be destroyed 100 years from March 31, 1956.

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

USCIS is working with NARA to develop a retention schedule for data contained within SIMS.

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

The data retained in SIMS supports adjudication decisions, and ultimately law enforcement uses, and protection of national security. Additionally, via an approved disposition and retention schedule for A-File and C-File Records, NARA has directed that the information be retained for a specified period. 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?

The application information collected by SIMS is primarily shared with DHS's US-VISIT Program via an interface with US-VISIT's Automated Biometric Identification System (IDENT). The

interface with US-VISIT/IDENT allows USCIS to obtain an enumerator for those individuals whose biometrics are captured. The enumerator is a unique identifier assigned to the individual based on core biographic and biometric data captured in SIMS.

Pursuant to the underlying Systems of Records Notice, USVISIT/IDENT will share the information with any other component in DHS where DHS determines that the receiving component has a need to know the information to carry out national security, law enforcement, immigration, intelligence, and other DHS-mission-related functions.

In addition, biographic data (name and date of birth) is used to conduct background checks via DHS Interagency Border Inspection System (IBIS). If derogatory information is found on the individual, additional data from SIMS may be shared with other DHS agencies (Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE)) for purposes of law enforcement and protection of national security.

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

In accordance with data sharing agreements between US-VISIT and USCIS, the data collected by SIMS and shared with US-VISIT's IDENT includes key biographic and biometric data on those applicants seeking an adoption or any adult involved in the adoption process that is required to be fingerprinted by USCIS, such as members of the adopting household other than the adopting parents. The key biographic and biometric data will enable US-VISIT to perform a fingerprint verification and validation and generate/assign an enumerator to an individual. US-VISIT will record the transaction with USCIS as an "encounter" which may be shared with other government organizations for law enforcement and intelligence purposes. The following data elements are stored in SIMS and transmitted between US-VISIT/IDENT and SIMS to employ the enumeration service:

- CIS Person Account Id
- Enumerator Number
- Date of Enumeration / Encounter
- Biometric Check Result
- Biometric Check Date
- Biometric Identity Status
- Expiration of Fingerprints
- Location where Fingerprints were captured
- Person First Name

- Person Middle Name
- Person Last Name
- Person Date of Birth
- Person Gender Code
- Organization Name (i.e., Agency Name)
- Organization Unit Name (i.e., Agency Office Name)
- Encounter ID
- Fingerprint Pattern Code (e.g., bandaged, missing/amputated, etc.)

All data contained within SIMS for an individual is made available to ICE and CBP upon request for law enforcement and national security purposes, or as otherwise required by those entities in the performance of their official duties and if there is a need to know.

4.3 How is the information transmitted or disclosed?

SIMS utilizes the Enterprise Service Bus (ESB)[3] to access Enumeration Services for sending and receiving information to and from IDENT. The primary purpose of the ESB is to enable system interconnection and information sharing within USCIS and between USCIS and other government agencies. ESB will enable business process integration between legacy and modern systems within USCIS and DHS. For USCIS, ESB technology will allow the USCIS to leverage key legacy systems and rapidly add new technologies (e.g. SIMS) at lower costs, and quickly integrate modern systems with legacy systems at a more rapid pace than has previously been achieved.

SIMS transmits information to the ESB via secured lines using Transmission Control Protocol/Internet Protocol (TCP/IP) as the communication protocol. Subsequently, the ESB utilizes TCP/IP protocols and methods to transmit information to IDENT.

If SIMS data is transferred on portable media or via email to authorized DHS employees, USCIS will use NIST-approved encryption to ensure that data is not tampered with en route and to prevent unauthorized personnel from viewing it.

In addition, government personnel and contractors must adhere to the OMB guidance provided in OMB Memoranda, 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. Contractors must also sign non-disclosure agreements.

[3] For privacy information related to the Enterprise Service Bus (ESB), refer to the USCIS PIA approved and published for the Enterprise Service Bus.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated. For example, if a decision was made to limit internal sharing to certain components because of privacy or other concerns, include such a discussion.

The primary risk of internal data sharing is unauthorized access to or disclosure of information contained within SIMS. To mitigate this risk, a number of business and system rules have been implemented. Access to SIMS is given only to a limited number of authorized internal users that need it to perform their official duties. All authorized users must authenticate using a userid and password. Lastly, through policies and procedures, DHS limits the use and access of all data in SIMS to the purposes for which it was collected.

A secondary risk of internal data sharing is that an individual may not be fully aware that their information will be used by DHS to conduct a background investigation. In order to mitigate this risk, USCIS provides a Privacy Act Statement on its applications. The application also contains a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…" To further mitigate this risk, USCIS is issuing this PIA and the associated System of Record Notice (SORN) for the SIMS Pilot.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

Information collected by SIMS may be shared with the DoS on a need to know basis in order to obtain decisions on adoption related cases. The DoS plays a role in the adoption process both domestically and abroad with regards to policy and operational development. Within the U.S., DoS provides country-specific information to prospective adoptive parents, and oversees bilateral agreements and international conventions related to inter-country adoption. In foreign locations, where USCIS does not have International Offices, U.S. embassies and consulates process and adjudicate adoption applications. Consular officers issue Immigrant Visas to all eligible beneficiaries after USCIS has granted the benefit, or return petitions to the USCIS as "not clearly approvable" when the case may need to be evaluated in light of new information.

USCIS may share the information collected by SIMS with the Federal Bureau of Investigation (FBI) as needed for FBI Name Check and FBI Fingerprint Check purposes. If an authorized representative from an external organization provides a valid mission requirement for viewing

contents of the SIMS data and can show proper credentials, USCIS may allow him/her to view it with a USCIS employee present.

USCIS may share information collected by SIMS with the Social Security Administration so that social security numbers may be issues. In addition, the SSA may seek information relating to the adopted child to assist it in its determination of an adopted child's eligibility for benefits.

5.2 What information is shared and for what purpose?

The data collected by SIMS and shared with DoS includes the information captured on the USCIS' Form I-600, *Petition to Classify Orphan as an Immediate Relative* and Form I-600A, *Application for Advance Processing of Orphan Petition*. The data collected on these forms includes information about individuals and organizations, such as addresses, phone numbers, family member names, citizenship status, marital status, social security numbers, dates of birth, places of birth, gender, height, biometrics, and results of background investigations.

USCIS may share an individual's biographical information with the FBI. The FBI will use this information to conduct a background check against their system, and will send the results (FBI Name Check Response) back to USCIS' Background Check Service (BCS)[4] system. USCIS uses the FBI Name Check Response during the adjudication process to determine an individual's eligibility for an immigration benefit.

5.3 How is the information transmitted or disclosed?

For the purposes of the pilot, USCIS will not provide direct access to SIMS to users outside of DHS. However, information contained within SIMS may be transmitted or disclosed to external organizations in one of two ways:

- DHS personnel may provide information contained in SIMS to external organizations who are co-located with DHS personnel who have access to the system; and
- USCIS may securely transfer encrypted SIMS data by email or other encrypted portable media (e.g., CD, thumb drive) when there is no direct access to SIMS. USCIS transfers the encrypted data to an authorized DHS employee who then allows an authorized representative from an outside government organization to view it. (See 5.4 and 5.5 for additional information.)

In addition, government personnel and contractors must adhere to the OMB guidance provided in OMB Memoranda, M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006

[4] For privacy information related to USCIS' Background Check Service, refer to the USCIS PIA for the Background Check Service, published on October 31, 2006.

setting forth the standards for the handling and safeguarding of personally identifying information. Contractors must also sign non-disclosure agreements.

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?

At this time USCIS does not have blanket sharing agreements or MOUs in place with external organizations to provide access to SIMS. USCIS will work with external organizations on a case-by-case basis. If an authorized representative from an external organization provides a valid mission requirement for viewing contents of the SIMS data and can show proper credentials, USCIS may allow him/her to view it with a USCIS employee present.

Currently, USCIS is bound by regulation (Title 22 of the Code of Federal Regulations (CFR) Part 104, International Trafficking in Persons: Interagency Coordination of Activities and Sharing of Information) to provide information to DoS for inter-country adoption purposes.

USCIS has existing MOUs with the FBI. The terms and conditions for the exchange of data for Name and Fingerprint Check purposes are covered in the MOUs between USCIS and the FBI and limit the use and re-dissemination of the information. The FBI does not share any information provided by USCIS for Name Checks and Fingerprint Checks.

5.5 How is the shared information secured by the recipient?

Representatives from external organizations may visit a USCIS office and view information contained within SIMS. They are shown only the portions of the data that they need. External representatives may not make copies but they may take notes. Each time data is viewed by an outside organization a non-disclosure form is completed and archived.

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

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. Contractors must also sign non-disclosure agreements. Any federal agency receiving this information is required to handle it in accordance with the Privacy Act and their applicable SORN.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to limit external sharing, include such a discussion.

The primary risk of external data sharing is unauthorized access to or disclosure of information contained within SIMS. To mitigate this risk, a number of business and system rules have been implemented. Access to SIMS is given only to a limited number of external users that need it to perform their official duties. All authorized users must authenticate using a userid and password. Lastly, representatives viewing the data must sign a non-disclosure agreement which outlines the limits and restrictions regarding use of the data. Information provided to external entities may not be further shared outside of those entities without the prior written consent of DHS.

Section 6.0 Notice

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

A SORN and PIA will be published for the Inter-country Adoption implementation of SIMS Pilot. Individuals who submit applications for adoption will be presented with a Privacy Act Statement (Appendix B) and a signature release authorization on each application related to adoption which will enable DHS to disclose information to other entities involved in the adjudication of the adoption application to include those performing home studies. In addition the system of records notices for the Central Index System (CIS)[5] and Background Check System (BCS)[6] both apply.

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

Individuals who submit applications for adoption will be presented with a Privacy Act Statement and a signature release authorization on each application related to adoption. The Privacy Act Statement details the authority and uses for information that the individual provides on the application. Each application also contains a signature certification and authorization to release any information from an individual's record that USCIS needs to determine eligibility. It is within the rights of the individual to decline to provide the required information; however, it will result in the denial of the individual's benefit request.

5 USCIS Central Index System (CIS) Federal Register reference: CIS/IDDMP 72 FR 1755-02
6 USCIS Background Check Service (BCS) Federal Register reference: BCS 72 FR 70413-02

On its applications, USCIS requires certain biographic information and may also require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision in granting or denying a USCIS benefit. The failure to submit such information would prohibit USCIS from processing and properly adjudicating the application and thus preclude the individual from receiving the benefit. Therefore, through the application process, individuals have consented to the use of the information for adjudication purposes, including background investigations.

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?

A Privacy Act Statement detailing authority and uses of information is presented to the individual. The application also contains a signature certification and authorization to release any information from an individual record that USCIS needs to determine eligibility, including biometric and biographic information.

All USCIS applications include a Privacy Act Statement and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…"

Consent is given for any use to determine eligibility, when the individual signs the application.

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

The collection of personally identifiable information is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk that an individual may not be fully aware that their information will be used to conduct a background investigation is associated with this particular collection of information. In order to mitigate this risk, USCIS provides a Privacy Act Statement on its applications. The application also contains a signature certification and authorization to release any information provided by the individual. To further mitigate this risk, USCIS is issuing this PIA and the associated SORN for the SIMS Pilot.

Section 7.0 Individual Access, Redress and Correction

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

In order to gain access to one's information stored in the SIMS database, a request for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to themselves are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his/her account number and/or the full name, date and place of birth, and notarized signature, and any other information which may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, FOIA/PA Request, 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 web site, located at www.uscis.gov.

An individual who 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 have an opportunity to correct their data during interviews otherwise they may submit a redress request directly to the USCIS Privacy Officer who refers the redress request to USCIS' Office of Field Operations or Office of International Operations. When a redress is made, the change is added directly to the existing information stored in SIMS. If an applicant believes their file is incorrect but does not know which information is erroneous, the applicant may file a Privacy Act request as detailed in Section 7.1.

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

Individuals are notified of the procedures for correcting their information on USCIS application instructions, the USCIS website, and by USCIS personnel who interact with them.

7.4 If no redress is provided, are alternatives available?

USCIS procedure for redress is provided to applicants as outlined in Sections 7.1 and 7.2.

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

Correction and redress rights are provided as set forth in Sections 7.1 through 7.4 above.

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.)

Access to SIMS will be limited to authorized DHS employees and contractors. Within that user group, SIMS will maintain five access roles: 1) Customer Service Representative, 2) Data Entry Clerk, 3) Officer, 4) Manager, and 5) System Administrator. If and when regular access is granted outside of DHS with external government agencies, this PIA will be updated and an MOU will be executed.

For the purposes of this pilot, the general public will not have access to SIMS.

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.

Yes. DHS contractors maintain SIMS and provide technical support. All access to SIMS follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

All contractors are required to undergo background checks and obtain favorable results. All IT contracts must contain Privacy Act compliance language before the award according to DHS contracting guidelines based on the Federal Acquisition Regulation (FAR) and other Executive Orders, public law, and national policy.

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

Yes. Access to SIMS is assigned based on the specific role of the user. Roles are created for each level of access required for individuals to perform their official duties. These roles include Customer Service Representative, Data Entry Clerk, Officer, Manager, and System Administrator. System Administrators assign these roles and their associated access based upon a user's need to know and level of security clearance.

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 SIMS. 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 SIMS is controlled via the Active Directory to authenticate users. (Active Directory is an agency-wide software tool that manages userids and passwords.) The SIMS uses Active Directory to authenticate the userid and password. Once authenticated, SIMS retrieves the role (i.e., Customer Service Representative, Data Entry Clerk, Officer, Manager, and System Administrator) and derives the appropriate permissions based on the role. System Administrators assign roles so that users have appropriate access to perform their particular job functions.

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

Roles are assigned by a System Administrator and are reviewed regularly to ensure that users have appropriate access to SIMS. Roles are stored in Active Directory and are used by SIMS to assign the appropriate permissions (see 8.4 above). Access is audited and audit logs are reviewed on a regular basis. Individuals who no longer require access are removed from the access list.

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

SIMS follows a system security plan that is in accordance with the USCIS systems lifecycle methodology. This plan is the primary reference that documents systems security responsibilities, policies, controls, and procedures.

The following security standards are employed by SIMS to prevent misuse of data:

- User Authentication – SIMS utilizes a security adapter to authenticate users through a third party authentication service.

- Encryption – SIMS is configurable to use encryption at multiple levels to ensure data confidentiality. Data is encrypted using SSL for transmission over the network between the client browser and Web server. As warranted, SIMS will be configured to utilize encryption between the Web server and application servers. Additionally, data is selectively encrypted at the field level in the database in accordance with the system design for securing data storage. Encrypting the data storage prevents attempts to view sensitive data directly from the database. If SIMS data is transferred on portable media or via email to authorized DHS employees, NIST-approved encryption will be used to ensure that data is not tampered with en route and to prevent unauthorized personnel from viewing it.
- Data Access Controls – SIMS uses view-level and record-level access control to manage user access to application functions and data. A view is a discrete set of functionality within the application. View-level access control determines the application functions that a user has access to based on the assignment of "responsibilities" which is a collection of views. Record-level access control assigns permissions to users, organization groups, and access groups to allow access to individual data items.
- Audit –SIMS employs two methods for auditing data:
    - At the record level, each record includes four fields to capture the date/time and user data creation and last updated.
    - SIMS uses an audit trail to capture who, when, and what changed for select data elements as identified in the system design.

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

All DHS system users complete mandatory annual computer security awareness training which addresses some privacy issues. Users will also complete SIMS training.

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

The system is built according to FISMA requirements. The Certification and Accreditation (C&A) process, as identified in the USCIS systems lifecycle methodology, will be conducted. The C&A process will be completed prior to the system being operational.

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

Access and security controls are established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users are broken into specific user roles with specific access rights. Audit trails are kept in order to track and identify unauthorized uses of system information. Data encryption is employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data is not compromised while in transmission. SIMS complies with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack and unauthorized information dissemination.

Section 9.0 Technology

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

SIMS is entirely made up of a configured Commercial-Off-The-Shelf (COTS) application purchased for use by USCIS. This application, Siebel Public Sector software, is an integrated suite of web-based applications designed for use by administrators and end users. Siebel Public Sector software provides an integrated foundation for complex case, service and agency management.

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

System designers and operational users of the system are working closely with privacy professionals to ensure compliance with the Privacy Act and the requirements of FISMA. The Transformation Program is working with a comprehensive Computer and Telecommunications Security (C&TS) Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. In addition, the Transformation Program follows the USCIS systems lifecycle methodology process, which is supplemented with information from DHS and USCIS security policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance.

9.3 What design choices were made to enhance privacy?

To protect against unauthorized disclosure, SIMS is designed to support discreet user roles and provide five levels of access to the system – Customer Service Representative, Data Entry Clerk,

Officer, Manager, and System Administrator. Access control rules are based on the user role, which reflects the need to know of the person accessing the files. These security requirements form the basis for the system security plan that is developed in accordance with the USCIS systems lifecycle methodology. The system records and prepares an audit trail for all transactions that create, update, request, or delete information from the system. The audit trail, which includes the date, time, and user for the each transaction, will be reviewed regularly.

Conclusion

The SIMS Pilot with Inter-Country adoptions provides a valuable service to USCIS' Transformation Program initiative, DHS, and its external data sharing partners by providing electronic access to data which was previously only available in hardcopy. It will also pilot Transformation's person-centric model which is designed to facilitate customer friendly transactions, track activities, and reduce identify fraud. While there are recognized privacy risks associated with the electronic collection, storage, and transmission of data, these risks are mitigated by technical safeguards and supporting policies and procedures. These mechanisms include: system design and controls; DHS policies and security programs; training; and clearly articulated data sharing guidelines and operating procedures.

Responsible Officials

Elizabeth Gaffin
USCIS, Privacy Officer
Department of Homeland Security

Approval Signature

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A – Proposed Operational Concept

Step	Pilot Description	Long-Term Description
Create or log-in to account	USCIS creates new or logs-in to an existing electronic account on behalf of the individual.	Individual creates new or logs-in to existing USCIS account electronically.
Request benefit	Individual files a paper application for a benefit (e.g. adoption or citizenship) with USCIS by sending to a centralized location.	Individual files an electronic application for a benefit (e.g. adoption or citizenship) with USCIS.
Create case and link information	Data Entry Clerk or Adjudicator creates a case in the system and links all relevant information.	System receives electronic application and automatically creates case and links all relevant information.
Complete background check	After case is created, adjudicator logs background check details and results to the individual's account.	After case is created, background checks are automatically executed and tied to the individual's account.
Distribute case	Supervisors manually distribute case to adjudicator based on workload and availability.	System automatically distributes case to adjudicator based on workload and availability.
Review case	Adjudicator reviews electronic case and supporting documentation.	Adjudicator reviews electronic case and supporting documentation.
Decide case	Adjudicator approves or denies case and electronically records case decision.	Adjudicator approves or denies case and electronically records case decision.
Issue notice or documentation	USCIS generates correspondence from the system and distributes to individual.	USCIS generates correspondence from the system and distributes to individual.
Submit supporting documentation	Individual or representative on behalf of applicant submits supporting documentation to USCIS.	Individual or representative on behalf of applicant submits supporting documentation electronically to USCIS.
Submit biometrics	Individual submits biometrics to USCIS upon completion at ASC.	Individual biometric information is automatically submitted to USCIS upon completion at ASC.

Appendix B – Privacy Act Notifications

Listed below are the respective Privacy Act Statements provided in the instructions section of each USCIS form related to an adoption case:

I-600A & I-600

8 U.S.C 1154 (a). Routine uses for disclosure under the Privacy Act of 1974 have been published in the Federal Register and are available upon request. USCIS will use the information to determine immigrant eligibility. Submission of the information is voluntary, but failure to provide any or all of the information may result in denial of the application.

N-600

USCIS will use the information and evidence requested on Form N-600 to determine your eligibility for the requested immigration benefit. We may provide information from your application to other government agencies.

N-600K

USCIS will use the information and evidence requested on Form N-600K to determine your eligibility for the requested immigration benefit. We may provide information from your application to other government agencies.