Privacy Impact Assessment
for the

Systematic Alien Verification for Entitlements (SAVE) Program

DHS/USCIS/PIA-006

August 26, 2011

Contact Point
Janice Jackson
Acting Privacy Branch Chief, Verification Division
United States Citizenship and Immigration Services
(202) 443-0109

Reviewing Officials
Donald Hawkins
Chief Privacy Officer
United States and Citizenship and Immigration Services
(202) 272-8000

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

Abstract

The Verification Division of the United States Citizenship and Immigration Services (USCIS) administers the Systematic Alien Verification for Entitlements (SAVE) Program. SAVE is a fee-based intergovernmental initiative designed to help federal, state, tribal, and local government agencies check immigration status for granting benefits, licenses, and other lawful purposes. Previously, USCIS documented the SAVE Program along with the E-Verify Program in the Privacy Impact Assessment (PIA) and System of Records Notice (SORN) of the Verification Information System (VIS), which is the technology that supports both programs. USCIS has conducted separate PIAs for the SAVE and E-Verify programs to assist the public in better understanding each program.

Overview

Background

The United States Citizenship and Immigration Services (USCIS) administers the Systematic Alien Verification for Entitlements (SAVE) Program. SAVE is a fee-based intergovernmental initiative designed to help federal, state, tribal, and local government agencies and licensing bureaus confirm immigration status information which includes status verifications by a federal, state, tribal, or local government agency, or by a contractor acting on the agency's behalf, to the extent that such disclosure is necessary to enable these agencies to make decisions related to: (1) determining of eligibility for a federal, state, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; or (5) any other lawful purpose.

A federal, state, tribal, or local government agency that provides a public benefit or license, or that is otherwise authorized by law to engage in an activity related to the verification of immigration status, may enroll in SAVE as a customer agency. By using SAVE, federal, state, tribal, and local customer agencies can request immigration status information in order to make a determination regarding the applicant's eligibility for a benefit or a license. It is important to note that SAVE does not make determinations on an applicant's eligibility for a specific benefit or license, but it does provide the necessary information to the agencies to allow them to make an informed decision prior to issuing benefits or licenses. The customer agency analyzes the SAVE response against the agency's own eligibility criteria to make an award determination. SAVE does not know the final outcome of the benefit adjudication.

SAVE has access to multiple immigration record systems from a variety of government agencies in order to confirm immigration status. All SAVE customer agencies must adhere to a Memorandum of Agreement (MOA) or Computer Matching Agreement (CMA), which include binding responsibilities regarding proper information usage and handling of SAVE information. The MOA also stipulates the terms for billing and payment. Relative to its billing and registration process, SAVE collects personally identifiable information (PII) such as the customer agency's point of contact name and professional contact information, as well as customer agency

and demographic information. SAVE staff may also collect sensitive information such as customer agency credit card information and other data relevant to the billing process.

Before an applying agency is accepted as a SAVE customer, it must first be cleared through an online registration process in which agencies are required to provide the legal authorities that allow them to administer benefits and verify citizenship or immigration status for those benefits. USCIS legal counsel reviews each application before it is approved.

Additionally, in administering the SAVE Program, the USCIS Verification Division may use information about customer agencies to conduct training and outreach marketing activities. These activities may require using information collected from customer agencies or commercially-available company mailing lists. SAVE may also use collected information to engage in customer service-oriented activities to improve customer agency relationships, such as outbound welcome calls, surveys, mass message distribution, and other quality assurance activities (e.g., complaints center). Inbound and outbound calls may be recorded and retained for training and quality assurance purposes. Information may also be used for monitoring and compliance activities, especially in connection with possible fraud, discrimination, or misuse and abuse of the SAVE system. These activities are essential to educate the public about SAVE and ensure proper usage of the program. Information may also be used for statistical analysis and recommending program enhancements.

A typical SAVE verification involves a registered federal, state, tribal, or local government benefit or license granting agency verifying the immigration status of an immigrant or non-immigrant. The immigration status is based on information from a state or U.S. government-issued document, such as a Permanent Resident Card (often referred to as a Green Card) or Employment Authorization Document. Before a SAVE customer agency can submit a query, the agency must collect certain information from the benefit or license applicant's immigration-related document. The verification process is document driven and requires the document's numeric identifier, e.g., Alien Number (A-Number). The document presented by the individual determines the verification process. SAVE verifies non-citizens and naturalized citizens. Native-born U.S. citizens are not subject to SAVE verification and would not possess approved documents, e.g., Lawful Permanent Resident Cards or Certificates of Naturalization. A customer agency will only query SAVE on individuals who are covered by the Immigration and Nationality Act (INA) and have appropriate documentation. In the vast majority of cases these are immigrants or non-immigrants, but they may also include naturalized or derived U.S. citizens.[1] Individuals presenting U.S. passports cannot be verified in SAVE because U.S. Passports cannot be used to initiate a SAVE query.

When a SAVE customer agency submits a query, SAVE queries various databases for matching records. These databases consist of the Department of Homeland Security (DHS) case management databases used for adjudicating immigration benefits, such as the Computer-Linked

[1] Naturalized citizenship is defined as the conferring, by any means, of citizenship upon a person after birth. Derived citizenship is defined as citizenship conveyed to children through the naturalization of parents or, under certain circumstances, to foreign-born children adopted by U.S. citizens, provided certain conditions are met.

Application Information Management Systems (CLAIMS 3 and CLAIMS 4) and the Department of Justice (DOJ) Executive Office Immigration Review (EOIR) System.

If SAVE locates a record pertaining to the applicant in any of these DHS databases, SAVE displays that data. The data displayed by SAVE depends on the customer agency's authority to use SAVE and the type of benefit the customer agency provides. For example, Departments of Motor Vehicles (DMV) are not authorized to receive an immigrant's sponsorship information and therefore would not receive it.

If SAVE is unable to find a record pertaining to the applicant, it displays a "Institute Additional Verification" message. The SAVE customer agency may initiate the additional verification procedure, which entails an in-depth query by USCIS Immigration Status Verifiers (Status Verifier) to determine the applicant's immigration status. At the point at which the "Institute Additional Verification" message is displayed, customer agencies are required to inform benefit applicants of the additional verification option and to pursue it if requested by the applicant. This is part of the MOA for all customer agencies.

Status Verifiers perform the additional verification queries and return responses to the customer agency electronically. The additional verification ensures that the Status Verifiers check appropriate DHS record systems and the DOJ's EOIR system. During second and third step verification, Status Verifiers have read-only access to information contained in immigration systems described in the attached appendices available through the Person Centric Query System (PCQS). Status Verifiers will only query this information to review applicant records. Each connected system provides a view of information related to immigrants and non-immigrants that is specific to the process or program managed by that connected system.

If the customer agency declines the second step additional verification, the process ceases. If the customer agency elects the second step, the process continues. If the second step search produces relevant information enabling verification of immigration status, SAVE provides an electronic notice to the inquiring customer agency. If SAVE is still unable to locate a record for the applicant during the second step, SAVE electronically notifies the customer agency to submit Form G-845, *Document Verification Request*, with a copy of the applicant's immigration documents, for a third step search.[2]

While each of the systems may also provide other capabilities, such as case management, adjudication updates, or background checks, Status Verifiers only use PCQS for second and third step verification to determine the immigration status of the applicant. In addition to conducting manual queries of databases for status verification, Status Verifiers may also request record corrections to the USCIS Central Index System (CIS) database by contacting the USCIS Records Division, as appropriate, so that status will be corrected for any future SAVE queries.

[2] If the submitted Form G-845 is incomplete, Form G-1120, Status Verification Return Checklist, may be sent to the inquiring customer agency. Form G-1120 includes an explanation of what information is missing in Form G-845. Also, if an unregistered, non-customer agency attempts to use SAVE, Form G-1120 is sent advising them to register, if eligible.

Other SAVE Verification Processes

The most recent Verification Information System (VIS) Privacy Impact Assessment (PIA) Update and the VIS System of Records Notice (SORN)[3] recognized the expanded scope of SAVE to include supporting customer agencies that conduct federal security clearance background investigations of third parties. A customer agency conducting a federal background investigation on an individual may use SAVE to verify the immigration status of that individual's family members, cohabitants, and other affiliates. For example, if a federal government customer agency selected an individual for a government position that requires a security clearance, the Office of Personnel Management (OPM) may use SAVE to verify immigration status information on that individual and any family members, cohabitants, and other affiliates as part of the security clearance process.

SAVE also assists in providing immigration status information for other lawful purposes. For example, the United States Armed Forces verifies status as part of its recruitment activities. Similarly, U.S. nuclear power plants may verify immigration status for security badges.

The REAL ID Act of 2005, Pub. L. No.109-13, 119 Stat. requires that any state seeking to be REAL ID compliant use the SAVE Program to verify the legal presence status of non-U.S. citizens requesting driver's licenses and state-issued identification cards. Many state DMVs already access SAVE to determine the status of non-citizens. In addition to verifying immigration status through traditional SAVE access methods, REAL ID DMVs may accomplish verification through the American Association of Motor Vehicle Administrators Network (AAMVAnet). The USCIS Enterprise Service Bus (ESB) is the electronic conduit through which AAMVAnet links to VIS. In some cases, a DMV may provide driver's license numbers to SAVE. SAVE does not retain this information.

Also by using AAMVAnet, REAL ID DMVs may verify passport data by linking to the ESB to connect to CBP Pass, administered by the U.S. Customs and Border Protection. By submitting only the date of birth of the passport holder and passport number, the passport information in the Department of State (DoS) database, Passport Information Electronic Records System, is queried. If there is a passport on record with information matching that provided by the DMV, a "Match" is returned. If no record is found, a "No Match" is returned. Under provisions of a Memorandum of Agreement between DHS and DoS, no passport data is transmitted to the DMV.

In addition, SAVE is currently developing the capability to use Photo Tool for those DMVs that access SAVE through AAMVAnet. When a DMV submits a query for verification of status using certain documents, SAVE retrieves currently available data from various sources and checks the Customer Profile Management System (CPMS) database to determine if a photo associated with the document the applicant presents is available. Other fields, such as date of birth, are also checked to avoid retrieving the wrong photo. If a photo is found, it is returned to the requestor's screen at the DMV along with the pertinent information from the database. The

[3] DHS/USCIS/PIA-006 Verification Information System and DHS/USCIS-004 Verification Information System SORN will be retired upon publication of the SAVE PIA and SORN.

DMV may use this information in their decision-making process for driver's license or ID card issuance. This process has not been finalized so it will be described more fully in a future PIA. Following the development of Photo Tool for DMVs accessing SAVE through AAMVAnet, SAVE intends to make it available to other agencies using other SAVE access methods.

Reasons for Publishing this PIA

Previously, DHS published the VIS single PIA and SORN, which addressed both SAVE and E-Verify. In addition, DHS published a PIA for the Person Centric Query System (PCQS), which supports both SAVE and E-Verify. DHS determined that publishing separate PIAs for SAVE and E-Verify incorporating appropriate information from both the VIS and PCQS PIAs would better assist the public in understanding these programs.[4] This PIA refers to SAVE when addressing programmatic issues and references to VIS and PCQS and the technologies that support the program. Upon publication of the SAVE PIA, the VIS PIAs will be retired. The PCQS PIAs will remain in effect because they provide a more detailed explanation of the service as part of the overall USCIS service-oriented architecture.

This PIA also elaborates on SAVE's expanded use of foreign passport numbers for non-immigrants from visa waiver countries. Foreign passport numbers will now be relied upon more frequently as an identifier because the U.S. Customs and Border Protection (CBP) no longer gives Form I-94W, Nonimmigrant Visa Waiver Arrival/Departure Form, to non-immigrants from visa waiver countries entering into the United States. The SAVE program previously relied on Form I-94W identification numbers to identify non-immigrants from visa waiver countries. Passport numbers were chosen because affected non-immigrants may not have acceptable DHS-issued documents, but in all cases should have their foreign passports at entry. Few travelers from visa waiver countries apply for the benefits administered by SAVE customer agencies.

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?

SAVE receives daily or real-time downloads from several DHS systems as described in Section 1.2. SAVE collects query and transaction information from the SAVE customer agencies. Much of this information pertains to individuals dealing with USCIS pursuant to INA, such as applicants for immigration benefits, petitioners, and non-immigrant visa holders. Information collected from the customer agency to facilitate verification of immigration status verification may include the following:

[4] DHS published PIAs for E-Verify in May and June of 2010. These are available at http://www.dhs.gov/privacy.

About the Individual (i.e., applicant)

- Receipt Number (issued by USCIS for applications for immigrant or nonimmigrant benefits)
- Alien Number
- Form I-94, Arrival-Departure Record Number
- Name (last, first, middle)
- Date of Birth
- Nationality
- Customer Agency-issued Case Number
- DHS document expiration date
- DHS Document Number
- Student Exchange and Visitor Information System (SEVIS) ID
- Foreign Passport Number
- U.S.-issued Visa Number
- Alias
- Social Security Number (in very limited circumstances using the Form G-845, Document Verification Request)
- Type of benefit the applicant is seeking

About the Customer Agency (e.g., federal, state, tribal, local, and other government agencies)

- Name of Agency
- Address
- Point of Contact
- Contact Telephone Number
- Authority to Issue Benefits
- Data Universal Numbering System (DUNS) Number (or Dun and Bradstreet Number)
- Tax Payer Identification Number
- Trading Partner Number
- Agency Locator Code

About the Agency Customer

- Name (last, first, middle)
- Phone Number
- Fax Number
- E-mail Address
- Customer ID for users within the Agency

Information Generated from Initial Verification

- Case Verification Number
- Immigration Status

Additional information is generated from and used in second and third step verifications. These additional verification steps use information from DHS databases, as well as databases from the U.S. DOJ and DoS. A listing of databases and data elements is provided in Appendix A, a description of the databases is provided in Appendix B, and a listing of system PIAs and SORNs is provided in Appendix C.

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

SAVE is supported by and uses information derived from individuals, customer agencies, VIS, other DHS agencies, DoS, and DOJ systems. The SAVE system receives daily downloads of relevant subsets of information about individuals coming before USCIS pursuant to the INA, to include applicants for immigration benefits, petitioners, and non-immigrant visa holders. Specific information received in these downloads is provided by the following DHS databases:[5]

- Arrival Departure Information System (ADIS)
- Central Index System (CIS)
- Computer-Linked Application Information Management System 3.0 (Claims 3)
- Computer-Linked Application Information Management System 4.0 (Claims 4)
- ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM)
- Enterprise Document management System (EDMS)
- Imagine Storage and Retrieval System (ISRS)[6]
- Marriage Fraud Amendment System (MFAS)
- Microfilm Digitization Application System (MiDAS)
- Refugees, Asylum, and Parole System (RAPS)
- Reengineered Naturalization Applications Casework System (RNACS)[7]
- Student and Exchange Visitor Identification System (SEVIS)

[5] Privacy Impact Assessments (PIA) and System of Record Notices (SORN) for DHS systems are on the DHS Privacy Web site at: http://www.dhs.gov/privacy.
[6] ISRS is scheduled to be decommission by early 2011 and replaced by the Customer Profile Management System.
[7] RNACS is scheduled to be decommissioned in late 2011.

Information about the Individual Benefit Applicant

SAVE receives information about applicants from the customer agencies. The subject of the query does not have direct access to SAVE. Instead, information about the individual is submitted by a SAVE customer agency.

The Customer Agency (i.e., federal, state, tribal, local, or other government agencies)

Customer agencies participating in SAVE provide data about themselves including the name of the agency, business address, phone number, and point of contact information, as well as SAVE customer contact information and data about the person being queried.

Some agencies use a single sign-on for all of their individual users. In these cases, SAVE will not collect information from individual users because individual users will appear as one agency user. In the case of single sign-on access to users, SAVE requires the agency to sign an addendum to the MOA which states that every user of the system must be assigned a unique identifier for internal identification. If requested, the agency will provide this information to SAVE to allow for a clear audit trail for all transactions.

A description of federal databases is provided in Appendix B.

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

Data about an individual is used to verify the immigration status of that individual to determine eligibility for benefits, credentials, and licenses issued by a federal, state, tribal, or local government agency. Data is also used for federal security background investigations and other lawful purposes. A variety of data is used for cross-referencing to ensure that data is accurate and current, to identify inconsistencies between or among databases, and to minimize fraud. Additionally, PII is collected from individual users of the system to provide accountability of system usage in the event of misuse and abuse of the system. Finally, SAVE data is used for registering agencies and other administration functions.

1.4 How is the information collected?

SAVE collects information about the customer agency and the users of SAVE directly from the agency, applicants of the customer agency, immigration status from other federal government systems, and as it relates to the misuse and abuse of the system. How this information is collected is described below:

Customer Agency Users: SAVE collects Information about the customer agency from the agency during the registration process. This information will include information about the agency along with information about the users of SAVE.

Applicants of Customer Agencies: SAVE collects information about a benefit applicant when the customer agency submits a query. SAVE compares that information to data found in DHS databases in order to provide appropriate responses to the requesting customer agency. Additional information about an applicant may be received during secondary verification.

Immigrant Status: SAVE collects information from daily or real-time downloads from several DHS systems and interfaces, as well as query and transaction information from SAVE customers. It also receives information from partnering agencies such as the Department of State and DOJ. A customer agency seeking to establish immigration status may do so by inputting information through secure means to include: 1) Secure File Transfer Protocols for batch transfers; 2) secure USCIS web site; 3) Web Services access;[8] or 4) by mailing Form G-845.

Misuse and Abuse of the System: SAVE also collects information in the course of its monitoring and compliance activities, especially in connection with determining the existence of fraud or discrimination in the use of the SAVE system. The USCIS Verification Call Center, law enforcement agencies, and the media also provide information to SAVE.

1.5 How will the information be checked for accuracy?

SAVE automatically provides the immigration status of an individual if the information entered through SAVE, during an initial verification query, matches a record housed in the SAVE database. Potential record inaccuracies are discovered when the record is queried and the customer agency provides information for comparison.

The accuracy of the responses depends on the accuracy of the data within the databases that share data with SAVE. If a discrepancy is encountered or if no record is found pertaining to an individual, status verifiers conduct a manual search of additional DHS databases to determine immigration status. If possible, status verifiers will verify the applicant's immigration status and request an update to the database. The applicant may be referred to a local USCIS office or to the appropriate record holding agency to resolve discrepancies that cannot be clarified through database or record searches.

With respect to information collected from individual applicants, it is incumbent upon both the applicants providing their information, as well as the customer agency performing the query, to verify the accuracy of information provided to SAVE. The SAVE Program provides a confirmation page to the customer agency to review prior to submitting the query.

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

Congress mandated that USCIS establish a system to verify the immigration status of individuals seeking government benefits or within the jurisdiction of the customer agency for any purpose authorized by law. Authority for having a system for verification of citizenship and immigration status of individuals seeking government benefits is governed by the Immigration Reform and Control Act of 1986 (IRCA), P.L. 99-603, 100 Stat. 3359; the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), P.L. 104-193, 110 Stat. 2105; Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility

[8] Web Services is a support service that allows SAVE customer agencies to access VIS information through a software interface.

Act of 1996 (IIRIRA), P.L. 104-208, 110 Stat. 3009; and the REAL ID Act of 2005, Pub. L. No.109-13, 119 Stat. 231.

All customer agencies participating in SAVE sign a MOA or CMA with SAVE.

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

VIS, the database supporting SAVE, is required to contain a large amount of PII to support its mission. Four privacy risks are identified due to this collection of the data.

Risk: The first risk is an unauthorized release of information, specifically a risk of returning unauthorized information to the customer agency.

Mitigation: To mitigate this risk SAVE customer agencies are categorized and coded according to the type of benefit they administer. Information is returned according to a customer agency's legally-authorized use. For example, a DMV would not receive sponsorship information about an individual. Only the minimum data required for accurate verification of driver's license eligibility is returned.

Risk: The second risk concerns data quality where inaccurate information may be attributed to an individual applying for a benefit.

Mitigation: To mitigate this risk, SAVE receives daily or real-time data enhancements and downloads from additional DHS and DOS systems to improve the completeness of SAVE data. DOJ's system is accessed directly. If, during initial verification, SAVE is unable to automatically verify an individual's status, Status Verifiers review the information and search other DHS databases to provide further verification so that an individual's status can be confirmed. When discrepancies are discovered during the second and third step manual verification, Status Verifiers may request corrections to the appropriate systems. SAVE is supported by an interconnected database of more than one hundred million selected immigration records from DHS and partner agencies. The uniqueness of each individual system and their combined diversity provides cross-references to minimize inaccurate information attributed to an individual. The result is fewer manual and second and third step verifications conducted by Immigration Status Verifiers. Further Status Verifiers also request record corrections to USCIS's Central Index System database, as appropriate.

Risk: The third risk is unauthorized customers registering to use SAVE.

Mitigation: To mitigate this risk, the SAVE Program staff conducts a manual review and approval of all applications to use SAVE. SAVE customer agencies register themselves online. In doing so, they may not clearly understand the SAVE definition for type of customer agency or benefit type administered. Incorrect selections during self-registration could result in extraneous information being returned from SAVE. To mitigate this risk, SAVE Program staff, as well as the USCIS legal department, review all initial registration applications against a checklist confirming the benefits the user agency claims to administer and its legal authority to do

so. If discrepancies are discovered, SAVE staff does not process the registration until the agency provides the correct information.

Risk: The fourth risk is PII being misused or an unintended use of the PII data.

Mitigation: To mitigate this risk, the SAVE Program ensures that data is used only for the purposes described in SAVE's PIA and SORN documentation. Other proposed uses are reviewed and put through a Privacy evaluation process as mandated by DHS Privacy Office. Additionally, the MOU or CMA signed by user agencies requires compliance with relevant sections of the Privacy Act and the Federal Information Security Management Act to safeguard and protect data from possible misuse.

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.

The primary use of the SAVE information is to provide immigration status information for any legally mandated purpose to federal, state, tribal, and local government customer agencies. The majority of customer agencies use SAVE to determine if applicants are entitled to receive the public benefits, licenses, or credentials they administer. For example, based on IRCA, customer agencies use SAVE when providing education and housing assistance, Medicaid, and unemployment benefits. PRWORA, by its definition of public benefits, allows customer agencies to use SAVE to determine the immigration status for purposes of licensing and loans. IIRIRA provides for customer agencies to use SAVE for any legal purpose such as background investigations and voter registration. In addition, the REAL ID Act of 2005 requires that any state choosing to be compliant with the Act utilize the SAVE Program to verify the immigration status of individuals claiming to be non-citizens before issuing them REAL ID compliant driver's licenses and identification cards.

Information in SAVE will only be used for SAVE verifications and for other administrative purposes aligning with the SAVE process, for such things as customer agency registration and relationship management, user accountability, program quality management, and monitoring and compliance activities.

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

SAVE uses both manual and automated comparisons of information to confirm immigration status. Analysts use the Compliance Tracking and Management System (CTMS), which supports all monitoring and compliance activities to ensure that customers follow proper procedures according to their signed agreements, as well as regulations. CTMS, which has its

own PIA and SORN,[9] collects and uses information necessary to support monitoring and compliance activities for researching and managing misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE. CTMS and SAVE produce reports and data extractions for evaluation by MPAs.

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

SAVE uses customer agency-oriented information such as Dun and Bradstreet numbers and tax identification numbers for billing purposes. SAVE may also use commercially available company mailing lists for outreach purposes.

The USCIS Office of the Chief Financial Officer requires the Dun and Bradstreet numbers (also referred to as a DUNS number) and tax identification numbers. They serve only as additional identifiers and are not used for cross-referencing. The DUNS numbers are also used by the U.S. Department of Treasury if they must collect owed payments from a delinquent user agency.

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.

Risk: The information contained in SAVE is used primarily to respond to inquiries from authorized customer agencies. Because SAVE collects PII pertaining to authorized customer agency points of contact (POCs) and accesses databases containing information about benefit seekers, there is a risk of unauthorized access to this information, use of this information in an unofficial capacity, or the presence of inaccurate information attributed to an individual.

Mitigation: To mitigate this risk, all customer agencies sign an MOA stating the intended use of the system and agreeing to the established security requirements. Each MOA contains provisions for training, policies, safeguarding of information obtained from the system, and procedures/instructions on the use of SAVE. Additionally, selected customer agencies must sign CMAs to ensure that information returned by SAVE is used and handled properly. The USCIS Verification Division Monitoring and Compliance Branch also evaluates and enforces adherence of user agencies to the agreements laid out in the MOA and CMA.

Section 3.0 Retention

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

3.1 What information is retained?

SAVE retains information collected from the various government databases described in

[9] CTMS PIA and SORN are available at http://www.dhs.gov/privacy.

the appendices and information on individuals applying for specific benefits when the benefit agency conducts a SAVE check. Additionally, the system maintains information about customer agencies, including the point of contact, the users, and the transaction history.

SAVE also retains information created by the SAVE Program such as the Case Verification Number. In processing second and third step verifications, applicants may provide copies of their identification documents that demonstrate identity and benefit eligibility. The majority of these hard copies are retained only for the period necessary to close the query and are then destroyed. Some hard copies of verified fraudulent documents may be retained for training and law enforcement purposes.

3.2 How long is information retained?

SAVE will retain information for 10 years from the date of the completion of the verification, unless the records are part of an on-going law enforcement investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud that is possible using SAVE (under 18 U.S.C. § 3291, the statute of limitations for false statements or misuse regarding passports, citizenship, or naturalization documents).

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

The retention scheduled N1-566-08-7 was approved by NARA on June 5, 2008.

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

Risk: All SAVE information is retained for a period of 10 years to coincide with the statute of limitations for most types of misuse or fraud that is possible using SAVE (under 18 U.S.C. § 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents). While the business justification for this retention is clear—pursuing SAVE fraud or misuse cases—the primary privacy risk associated with retaining the information for 10 years is that the information might be misused.

Mitigation: To mitigate this risk, the SAVE Program has a policy to retain only minimum information and to use technical controls that limit use and access to SAVE information. By policy, this information may only be used for verifying immigration status or for purposes that directly support the program such as prevention of misuse and fraud, program analysis, outreach, quality assurance, and customer service. Furthermore, the information in VIS, the underlying technology solution for SAVE, is purely transactional and individuals with access to the system have procedural and technical limitations that prevent them from searching the database for such things as previous verifications. For example, most customer agencies do not

have the ability to search VIS for closed cases. The SAVE Program has also developed monitoring and compliance capabilities to detect and reduce potential misuse of SAVE information.

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?

When potential fraud or misuse is indicated by SAVE information, this information may be shared, on a case-by-case basis, with DHS internal law enforcement organizations such as Immigration Customs Enforcement (ICE). For example, information could be shared with ICE if it were discovered that an Alien Number is used repeatedly in ways that are inconsistent with one legal individual using his own Alien Number. In these cases, SAVE shares only the information required to pursue an investigation into the potential fraud or misuse. Several DHS organizations are customers of SAVE and have access to information in response to their queries.

4.2 How is the information transmitted or disclosed?

All internal sharing is conducted over a secure DHS electronic interface. 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 PII. Contractors must also sign non-disclosure agreements that require them to follow departmental transmission and disclosure limitations. All data shared between agencies is transmitted or disclosed via secured communications.

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.

Risk: The main risk associated with internal information sharing is unauthorized access to PII.

Mitigation: To mitigate this risk, SAVE only shares information internally for law enforcement purposes regarding potential fraud or misuse of SAVE. USCIS limits data sharing to only those DHS components that have a need to know and put the information to uses that are compatible with the SAVE System of Record Notice (SORN).[10] DHS enforces the requirement of annual privacy and computer security training, which teaches how to handle and safeguard PII.

[10] The SAVE SORN (DHS/USCIS-004) will be published in conjunction with this PIA.

In addition, USCIS employees are required to review the responsibility of handling of sensitive and non-sensitive PII in Management Directive (MD) 140-001.

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?

Many SAVE customer agencies are external to DHS. Over 500 federal, state, tribal, and local government agencies currently use SAVE to receive immigration status information in response to their queries.

SAVE may also provide data to the Department of Justice (DOJ) or other law enforcement agencies in the case of an investigation or other legal matter related to the use of SAVE. The general purpose of responding to such matters is within the DOJ's jurisdiction to include investigation of allegations of immigration fraud, discrimination, and other misuses of SAVE.

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.

The instances of external sharing are compatible with the purpose of SAVE and are appropriately covered by routine uses in the SAVE SORN. In addition, sharing with SAVE customer agencies are covered by MOAs and CMAs, as appropriate. External sharing for law enforcement purposes to assist in the investigations of fraud, discrimination, and misuse cases is fully within the purpose of the original collection and supported by routine uses E, G, and H, of the SORN.

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

Besides sharing information with customer agencies to verify immigration status, SAVE may also share information for law enforcement purposes such as fraud and identify theft issues. The method of sharing and protections involved in that sharing will depend on the particular case. For example, information indicating that a single Alien Number has been used hundreds or thousands of times across the United States in a short period of time may require an electronic extraction of information that will be protected with encryption and securely transmitted electronically to the responsible law enforcement officer(s) working the potential case. The

extraction would be required to comply with all DHS and federal requirements including the Office of Management and Budget (OMB) Memorandum 06-16. Alternatively, a single SAVE transaction that appears to indicate fraud or misuse may be extracted in hard copy and delivered directly to the responsible law enforcement officer working the potential case.

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

Risk: There are privacy risks of the unintended use and the protection of PII when sharing information with the external entities in that information may be used to commit fraud or identity theft.

Mitigation: To mitigate these privacy risks, all SAVE customer agencies must adhere to MOAs and/or CMAs which stipulate binding responsibilities regarding safe handling of information, minimum security standards for electronic transmissions, and breach incident notification. These provisions are compliant with requirements of the Federal Information Security and Management Act, relevant OMB guidance, and DHS Sensitive Systems Policy 4300A.

Risk: There is a risk in sharing information with external organizations in that authorized users may misuse the information or unauthorized users may gain access to it. However, external sharing for law enforcement purposes to assist in the investigations of fraud, misuse, and discrimination cases is fully within the purpose of the original collection and supported by routine uses described in the SAVE SORN publishing concurrently with this PIA.

Mitigation: To mitigate this risk, sharing only takes place after DHS determines that the receiving component or agency has a need-to-know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this SORN.

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?

In many cases, notice is directly given to the individual applicants or benefit-seekers of SAVE customer agencies. The Small Business Administration collects information after receiving the applicant's written consent. Additionally, the MOA signed by all SAVE customer agencies requires them to adhere to the Privacy Act. The original MOA is a static document and binding as long as the customer agency uses SAVE. The MOA does, however, include a billing addendum that changes with each fiscal year.

There may be instances when the only notice will be through the publication of a PIA and an accompanying SORN. In some cases, federal agencies, such as OPM, will determine immigration status through SAVE, not only for a federal security clearance or public trust investigation subject (who has been given notice and provides consent based on agreeing to the background investigation), but also for family members, cohabitants, and other affiliates of the subject. OPM does not provide these individuals with the opportunity to consent, and these individuals will receive notification only through this PIA and accompanying SORN. This limited notification is justified based on national security concerns associated with individuals who will be granted security clearances or public trust positions.

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

Yes, applicants have the opportunity and/or right to decline to provide information to the customer agency from which they are seeking a benefit. However, declining or providing incomplete information may prevent SAVE's ability to verify their status, which ultimately may result in disqualification for the benefit the individual is seeking.

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

No, individuals do not have the right to consent to particular uses of the information. SAVE may provide information to customer agencies to support any lawful purpose including background investigations. The agency may give the individual clear notice at the time of application that failure to provide immigration status information may result in a determination of ineligibility for a particular benefit.

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.

Risk: There is a risk that when individuals apply for a benefit from SAVE customer agencies that the individual may be unaware of what sort of information is gathered and what is done with that information.

Mitigation: To mitigate this risk, each customer agency is responsible for informing individuals that the information they provide is collected to determine whether they are eligible for public benefits, licenses, or credentials. Federal customer agency applications will contain a privacy notice and statement where the individual authorizes the benefit-issuing customer agency to release any information from the application as needed to determine eligibility for benefits. State and local customer agencies may contain a privacy notice and statement, but such a notice is not necessary to enroll in SAVE. In addition, individuals may be advised that the information provided may be shared with other federal, state, local and law enforcement and regulatory

agencies during the course of the investigation. The SAVE SORN also provides additional notice to individuals by specifying the routine internal and external uses to which the information may be used. The SORN further indicates that information is maintained and destroyed according to the principles 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.

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?

Individuals may request access to their information by submitting a written Privacy Act request to USCIS clearly marked "Privacy Act Request" at the following address:

National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

Requesters are required to provide their A-Number and/or full name, date, and place of birth, and return address.

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

Individuals should direct all written requests to contest or amend their information reviewed by SAVE, with appropriate proof of identity, class of admission, and other relevant identifying information, as well as a statement about the incorrect information to the FOIA/PA Officer at the address provided in Section 7.1. Depending on the originating source of information, the request may be satisfied within USCIS or the individual may be referred to the appropriate record holding agency (e.g., Customs and Border Protection for the Nonimmigrant Information System and Border Crossing Information). If the source of data is from a USCIS download (e.g., CIS) and SAVE confirms the data is incorrect, by comparing the documents with the information in the SAVE database and cross referencing other VIS databases, SAVE will contact the appropriate system owner recommending that the data be corrected. Alternatively, the individual may make an appointment via INFOPASS located on the USCIS website to visit a USCIS District Office and request that a Level 1 Immigration Service Officer make the change. When appearing for the appointment, the person should provide accompanying supporting documentation, including proof of identity, class of admission, and other relevant identifying information. SAVE customer agencies may change their profile information directly within the VIS application.

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

The PIA and SORN for SAVE provide individuals with guidance for correcting information. Additionally, benefit-issuing agencies also provide instructions for correcting information with SAVE.

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

Formal redress is provided to individuals in accordance with the above sections 7.1 and 7.2.

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

Risk: The main risk regarding redress is that the right may be limited by Privacy Act exemptions. The redress and access measures offered by SAVE are appropriate given the purpose of the system.

Mitigation: To mitigate this risk, the second and third step verification options give individuals opportunities, during and after the completion of the benefits application process, to correct information they have provided to USCIS and/or the agencies from which they seek benefits.

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?

The SAVE Program requires potential enrollees and customer agencies to register for participation in the SAVE Program and sign a MOA or CMA. Once the required documentation is submitted, all users are required to complete a web-based training course that explains functionality and security requirements.

8.2 Will Department contractors have access to the system?

Yes, contractors will have access to SAVE. All contractors shall go through a suitability and personal clearance process before they can access the SAVE system. Appropriate non-disclosure agreements are signed by contractors. Additionally, all contractors are required to take security and privacy training annually as described in the section below.

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

SAVE internal users take the mandatory, annual DHS Computer Security Training and USCIS Privacy Awareness Training. Additionally, staff who administer the SAVE Program take special, supplemental training. External SAVE users take on-line tutorials explaining the SAVE Program. The tutorial also covers the procedures and policies associated with the use of SAVE and also includes Privacy.

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

Yes, VIS, as the underlying technology supporting SAVE has been Certified and Accredited and received a full authority to operate (ATO) in April 2008. This ATO expires April 2011, or before April 2011 if significant changes are made to VIS.

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

SAVE has implemented a broad range of technical, operational, and physical security measures to protect the system and its information. These security measures include access controls for both internal and external customers, such as account names and passwords to access SAVE. SAVE has an automated mechanism to ensure that users change their passwords at specified intervals. User accounts are locked after several failed attempts to logon. SAVE protects against password re-use. Additionally, inactive SAVE sessions timeout and require users to log in again. Other examples of security controls include:

- Password data is encrypted within the system;
- SAVE is located within a multi-layered firewall architecture;
- A robust set of security controls that meet DHS System Security Policy requirements are documented and verified through the certification and accreditation process;
- SAVE uses HTTPS protected communications during all data transmissions between the client workstation and the system;
- SAVE passwords are encrypted when making database connections; and
- Procedures are in place to ensure that any potential breaches of information are reported within one hour of being found.

SAVE has a comprehensive audit trail tracking and maintenance function that stores information on users who submit queries, when the query was processed, what the response was, who receives the response, and when the response was received. The audit logs have restricted access based on user roles. These logs are external to system administration access methods and protected from modification. These audit logs are periodically reviewed for monitoring user

activity. Customer agencies are required to abide by all security requirements as agreed to when they enrolled in SAVE. Attempts to evade the security controls can result in loss of access to SAVE.

Some agencies use a single sign-on for all of their individual users. In these cases, SAVE will not collect information from individual users because individual users will appear as one agency user. In the case of single sign-on access to users, SAVE requires the agency to sign an addendum to the MOA which states that every user of the system must be assigned a unique identifier. If requested, the agency provides this information to SAVE to allow for a clear audit trail for all transactions.

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?

Risk: There is risk that users may be unauthorized to access information.

Mitigation: SAVE mitigates the risk associated with user access to information by requiring program-specific training before system access is granted. SAVE is able to monitor use of the system. SAVE provides the customer agency administrator with the ability to assign and track user identification numbers and passwords; SAVE can also track these user identifiers. Additionally, there are a few customer agencies using single user sign-on. As applicable, new MOAs are signed based on DHS's Interface Control Agreement requiring that both DHS and the customer agency will be able to identify the customer agency user for a verification transaction. SAVE also requires the agency to sign an addendum to the MOA which states that every user of the system must be assigned a unique identifier. When requested, the agency must provide this information to SAVE to allow for a clear audit trail for all transactions. Additionally, responses to queries are tailored based upon agency mission requirements, providing each user with only the information necessary for their needs. DHS requires all employees, including SAVE users, to complete mandatory, annual DHS Computer Security Training and Privacy Awareness Training.

Risk: There is risk that users may alter SAVE data.

Mitigation: SAVE mitigates concerns about data alteration by users by providing all external users with "read-only" access. SAVE is also able to monitor access to SAVE by the designated users to identify any unusual activity or access.

Risk: There is a risk that unauthorized users may access PII.

Mitigation: SAVE mitigates concerns about unauthorized access to PII by monitoring for accounts that have not been used for long periods. SAVE brings such accounts to the attention of the customer agency for possible termination of the accounts.

Risk: There is a risk that there may be unauthorized agent users in the system.

Mitigation: SAVE mitigates the risk of unauthorized agent users by requiring all agencies to sign MOAs agreeing to abide by the stipulated use and access policies before granting access to the system. Additionally, data is only provided back to the originator or designee of the requesting agency.

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?

The SAVE program is comprised of an underlying technical infrastructure and operational policies and procedures for the verification of immigration status. VIS, as the supporting technology, is composed of databases and web services, and communication and security infrastructure.

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

SAVE is at the operations and maintenance stage of the DHS system development life cycle.

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

The SAVE application is a web-based service/application provided via Internet.

Risk: SAVE inherits privacy risks associated with applications available via Internet e.g., session hijacking, network sniffing, and exploitation of vulnerable web services.

Mitigation: These risks are mitigated to an acceptable level by implementing security controls per NIST and OMB guidelines as documented in relevant security plans and vetted through the Certification and Accreditation process.

Responsible Officials

Janice Jackson
Acting Chief, Privacy Branch
U.S. Citizenship and Immigration Services
Verification Division
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Information Generated from Second and/or Third Step Verifications (Includes Initial Verification Data) and Quick References

Status Verification System-provided information, as a result of the verification process under SAVE using Form G-845, Document Verification Request

- Case Verification Number
- Record in VIS database as outlined above, including pertinent information from CIS, SEVIS and CLAIMS 3 and with the exception of the biometric information (photograph) from CPMS.
- Immigration status (e.g. Lawful Permanent Resident)
- Employment eligibility information (depending on the document submitted). For example, for the Department of Labor, employment authorization history for past 18 months is provided
- Certain types of SAVE referrals may require returning information about whether an individual is on Order of Supervision, entry and parole information, and/or Affidavit of Support information.

Person Centric Query System (PCQS) – All personal information regarding an applicant's status is uploaded from various databases such as:

- Central Index System (CIS)
- Computer-Linked Application Management Information System 3.0 (CLAIMS 3)
- Computer-Linked Application Management Information System 4.0 (CLAIMS 4)
- Customer Profile Management System (CPMS)
- DOS Consular Consolidated Database (DOS-CCD)
- ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM)
- Executive Office of Immigration Review System (EOIR)
- Marriage Fraud Amendment System (MFAS)Microfilm Digitization Application System (MIDAS)
- National File Tracking System (NFTS)
- Nonimmigrant Information System and Border Crossing Information (NIIS and BCI)

- Refugees, Asylum, and Parole System (RAPS)
- Reengineered Naturalization Applications Casework Systems (RNACS)
- Immigration Customs and Enforcement (ICE) Student Exchange Visitor Information System (SEVIS)
- TECS System: CBP Primary and Secondary Processing (TECS)

Immigration Status Information Collected from DHS, DOJ, and DOS Systems (Sorted by Commonly Used Name Acronym)

United States Visitor and Immigrant Status Indicator Technology (US-VISIT)'s Arrival Departure Information System (ADIS)

- Last Name
- First Name
- Date of Birth
- Country of Citizenship
- Sex
- Passport Number
- Airline and Flight Number
- Country of Residence
- City Where Boarded
- City Where Visa was Issued
- Date Visa Issued
- Address While in United States
- Port of Entry

USCIS's Central Index System (CIS)

- Alien Number
- Last Name
- First Name
- Middle Name
- Date of Birth
- Date Entered United States
- Country of Birth

- Class of Admission
- File Control Office Code
- Social Security Number
- Form I-94 Number
- Office Code Where the Authorization Was Granted
- Employment Authorization Card Information
- Lawful Permanent Resident Card Information
- Naturalization Certificate Number
- EOIR Information, if in proceedings

USCIS's Computer-Linked Application Information Management System Version 3 (CLAIMS 3)

- Receipt Number
- Alien Number
- Last Name
- First Name
- Middle Name
- Address
- Social Security Number
- Gender
- Date of Birth
- Country of Birth
- Class of Admission or Type of Visa
- I-94 Number
- Employment Authorization Information
- Lawful Permanent Resident Information
- Date of Entry
- Valid-To Date
- Petitioner Internal Revenue Service Number
- Attorney Name
- Attorney Address

USCIS's Computer-Linked Application Information Management System Version 4.0 (CLAIMS 4)

- Alien Number
- Social Security Number
- Last Name
- First Name
- Middle Name
- Birth Date
- Birth Country
- Nationality
- Gender
- Naturalization Verification (Citizenship Certificate Identification ID)
- Naturalization Verification (Citizenship Naturalization Date/Time)
- Address

USCIS's Customer Profile Management System

- Receipt Number
- Alien Number
- Last Name
- First Name
- Middle Name
- Date of Birth
- Country of Birth
- Form Number, for example Form I-551 (Lawful Permanent Resident card) or Form I-766 (Employment Authorization Document)
- Expiration Date
- Photograph

Department of State (DOS)'s Consular Consolidated Database (DOS-CCD)

- Name
- Date of Birth
- Passport Number

- Visa Control Number
- FOIL Number
- Alien Number
- Photograph

ICE's ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM)

- Alien Number
- Name
- Marital Status
- Date of Birth
- Age
- Sex
- Country of Birth
- Country of Citizenship
- Date of Entry
- Class of Admission
- Social Security Number
- Federal Bureau of Investigation Number
- Case History
- Alerts
- Case Summary Comments
- Case Category
- Date of Encounter
- Encounter Information
- Custody Actions & Decisions
- Case Actions & Decisions
- Bonds
- Photograph

USCIS's Enterprise Document Management System (EDMS)

All Information Contained in an Individual's A-File, including, but not limited to:

- Alien Number
- Last Name

- First Name
- Middle Name
- Date of Birth
- Date Entered United States
- Country of Birth
- Class of Admission
- Social Security Number
- Form I-94 Number
- Naturalization Information and Certificate
- Photograph
- Marriage Information and Certificate

Department of Justice Executive Office Immigration Review System (EOIR)

- Name
- Alien Number
- Address
- Nationality
- Decision memoranda, investigatory reports and materials compiled for the purpose of enforcing immigration laws, exhibits, transcripts, and other case-related papers concerning aliens, alleged aliens or lawful permanent residents brought into the administrative adjudication process

USCIS's Marriage Fraud Amendment System (MFAS)

- Individual's
    - Name (Last, First, Middle)
    - Date of Birth
    - Country of Birth
    - Country of Citizenship
    - Class of Admission
    - Date of Admission
    - Alien Number
    - Receipt Number
    - Phone Number
    - Marriage Date and Place

- Spouse's
    - Name (Last, First, Middle)
    - Date of Birth
    - Country of Birth
    - Country of Citizenship
    - Class of Admission
    - Date of Admission
    - Alien Number
    - Receipt Number
    - Phone Number
    - Marriage Date and Place
    - Naturalization Date and Place
- Children's
    - Names (Last, First, Middle)
    - Date of Birth
    - Country of Birth
    - Class of Admission
    - Alien Number
- Employer
    - Name
    - Address
    - Supervisor's Name
    - Supervisor's Phone Number

USCIS's Microfilm Digitization Application System (MiDAS)

- Name
- Alien Number
- Date of Birth
- Citizenship Number

USCIS's National File Tracking System (NFTS)

- Alien Number
- File Location

USCIS's Refugees, Asylum, and Parole System (RAPS)

- Class of Admission
- Country of Birth
- Date of Birth
- Date of Entry
- Current Status
- Asylum Applicant Receipt Date

USCIS's Reengineered Naturalization Applications Casework System (RNACS)

- Alien Number
- Last Name
- First Name
- Middle Name
- Birth Date
- Birth Country
- Gender
- Nationality
- Naturalization Verification (Citizenship Naturalization Date/Time)
- Naturalization Verification (Citizenship Certificate Identification ID)
- Immigration Status (Immigration Status Code)
- Address

Immigration and Customs Enforcement (ICE)'s Student and Exchange Visitor Identification System (SEVIS)

- Student and Exchange Visitor Identification Number (SEVIS ID)
- Last Name
- First Name
- Middle Name
- Date of Birth
- Country of Birth
- Class of Admission
- I-94 Number
- Date of Entry
- Valid To Date

- Social Security Number
- Nationality
- Gender
- Student Status
- Visa Code
- Status Change Date
- Port of Entry Code
- Non Citizen Entry Date
- Status Code
- Program End Date

Quick Reference of SAVE Systems and their Use for Each Step of Verification (Sorted by Commonly Used Name Acronym)

Initial Verification (also used during Second and Third Step Verification)

- Central Index System (CIS)
- USCIS's Computer-Linked Application Information Management System Version 3 (CLAIMS 3)
- USCIS's Computer-Linked Application Information Management System Version 4.0 (CLAIMS 4)
- USCIS's Image Storage and Retrieval System (ISRS)
- USCIS's Reengineered Naturalization Applications Casework System (RNACS)
- Immigration and Customs Enforcement (ICE)'s Student and Exchange Visitor Identification System (SEVIS)

Second and Third Step Verification

- United States Visitor and Immigrant Status Indicator Technology (US-VISIT)'s Arrival Departure Information System (ADIS)
- Department of State (DOS)'s Consular Consolidated Database (DOS-CCD)
- ICE's ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM) USCIS's Enterprise Document Management System (EDMS)
- Department of Justice's Executive Office of Immigration Review System (EOIR)
- USCIS's Marriage Fraud Amendment System (MFAS)
- USCIS's Microfilm Digitization Application System (MiDAS)
- USCIS's National File Tracking System (NFTS)
- USCIS's Refugees, Asylum, and Parole System (RAPS)

Appendix B

Description of Federal Government Databases

- **Arrival Departure Information System (ADIS):** ADIS contains information on individuals arriving and departing at United States ports of entry. This information includes biographic information from passenger manifests and Forms I-94. SAVE uses this information to verify an individual's eligibility to be received public benefits, licenses, or credentials. Status Verifiers use ADIS as part of the secondary immigration status verification for SAVE.

- **Central Index System (CIS):** CIS contains information on the status of 57 million applicants/petitioners seeking immigration benefits to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., aliens who have been issued employment eligibility documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). Status Verifiers will use CIS as part of the immigration status verification for SAVE.

- **Computer-Linked Application Management Information System 3.0 (CLAIMS 3)**: CLAIMS 3 is a mainframe database centered major application that supports processing of USCIS applications and petitions for various immigrant benefits (e.g. change of status, employment eligibility, extension of stay, etc). It supports case management for and adjudication of all USCIS benefits except naturalization and citizenship. Status Verifiers will use CLAIMS 3 as part of the immigration status verification for SAVE.

- **Computer-Linked Application Information Management System Version 4.0 (CLAIMS 4):** CLAIMS 4 was developed by the Immigration and Naturalization Service (INS) to provide immigration status verification information and to assist in the processing applications related to naturalization or attaining U. S. citizenship. Status Verifiers will use CLAIMS 4 as part of the secondary immigration status verification for SAVE.

- **Customer Profile Management System (CPMS):** CPMS is the new repository of all digitized biometric data in USCIS. It stores biographic and biometric data used for Forms I-131 (Application for Travel Document); I-765 (Application for Employment Authorization); and I-551 (Alien Registration Card or Green Card). Status Verifiers will use CPMS as part of the immigration status verification for SAVE.

- **Department of State Consular Consolidated Database (DOS-CCD):** DOS-CCD is used by consular personnel as a resource for verifying prior visa issuances/refusals. It is also used by consular management for statistical reporting. Status Verifiers will use DOS-CCD as part of the secondary immigration status verification for the SAVE program. While the data from DOS-CCD will be used for verification, it will not be stored in VIS.

- **ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM):** EID contains biographic and case information on aliens encountered and booked in Immigration and Customs Enforcement (ICE) and other DHS component enforcement actions. Status Verifiers will use EID as part of the secondary immigration status verification for the SAVE program. Information from EID is required by the Status Verifiers to help determine whether an individual may not be eligible for employment, government benefit, credential, or other reason for which they are having their immigration status verified in the first place. DHS components collect the information in EID during enforcement or administrative actions. Its use for verification of immigration status follows because in all cases that the verification is performed, eligibility may be contingent on not having been the subject of an enforcement action.

- **USCIS Enterprise Document System (EDMS):** EDMS is a web-based system that allows users to view, search, and add comments to digitized immigration records or A-files. EDMS can consolidate digitized A-Files, while allowing users to display primary and secondary A-Files.

- **Executive Office Immigration Review System (EOIR):** This Department of Justice system contains information pertaining to aliens and alleged aliens brought into the immigration hearing process, including certain aliens previously or subsequently admitted for lawful permanent residence. Status Verifiers will use EOIR as part of the immigration status verification for the SAVE Program when there is a question of immigration status. Information from EOIR is required by the Status Verifiers in order to help determine whether an individual may be eligible for benefits, or other reasons for which they are having their immigration status verified in the first place. Its use for verification of immigration status follows because in all cases that the verification is performed, eligibility may be contingent on not having been the subject of an enforcement action.

- **Marriage Fraud Amendment System (MFAS):** The Marriage Fraud Amendment System (MFAS) supports and maintains casework resulting from the Immigration Marriage Fraud Amendment Act (MFA), which became law on November 10, 1986. MFAS allows users the ability to process and control applications and petitions to grant Conditional Permanent Resident (CPR) status and Permanent Resident (PR) status, and to identify and terminate the CPR status of aliens who acquired this status fraudulently or who have not removed this status during the designated time period that the law requires. Status Verifiers will use MFAS as part of the secondary immigration status verification for the SAVE program. While the data from MFAS will be used for verification, it will not be stored in VIS.

- **Microfilm Digitization Application System (MiDAS):** MiDAS is an image-based search and retrieval application of digitized alien records on individuals who entered the U.S. between 1906 and 1975 (50-60 million records). MiDAS allows the USCIS Office of Records to achieve a more effective search result and improved customer service. When digitization of all files is complete, the MiDAS database will hold over 80 million records including Master Index, Flex-O-Line, A-files,

Citizenship/Naturalization files (C-files, 129, 3904, OM, etc), file locator information cards, and other historical records. Status Verifiers will use MiDAS as part of the immigration status verification for SAVE.

- **National File Tracking System (NFTS):** NFTS provides a centralized, automated, mechanism for determining the location of a physical A-File and associated Receipt Files. NFTS supports the Records requirement to track files at the local level, as well as the national level. It is designed to support the Records mission and to provide efficient access to high-quality immigrant information by maintaining an accurate file inventory. Status Verifiers will use NFTS as part of the immigration status verification for the SAVE program in order to locate files.

- **Refugees, Asylum, and Parole System (RAPS):** RAPS contains biographic information collected for USCIS Form I-589, Asylum Application. Status Verifiers use RAPS as part of the secondary immigration status verification for SAVE. Information from RAPS is required by the Status Verifiers in order to help determine whether an individual is ineligible for employment. DHS components collect the information in RAPS when an applicant for asylum completes a Form I-589. Its use for verification of immigration status follows because asylum brings with it access to certain benefits.

- **Reengineered Naturalization Applications Casework Systems (RNACS):** RNACS provides full case tracking and management capability for naturalization casework including assignment of cases to Case Control Offices (CCO); queuing of cases for appropriate actions, scheduling interviews and oath ceremonies; editing transactions; reporting; and production of correspondence. Status Verifiers will use RNACS as part of the immigration status verification for SAVE.

- **Student and Exchange Visitor Identification System (SEVIS):** SEVIS maintains information on non-immigrant students and exchange visitors (F, M, and J Visas) and their dependents, and also on their associated schools and sponsors. SEVIS enables DHS to maintain current information and facilitate oversight relating to nonimmigrant foreign students and exchange visitors during the course of their stay in the U.S. SAVE accesses information from SEVIS and will use the information for primary verification of immigration status for SAVE. Status Verifiers will use SEVIS as part of the immigration status verification for SAVE.

Appendix C

Links to PIAs and SORNs of databases assessed by the SAVE Program
(Sorted by Commonly Used Name Acronyms)

- United States Visitor and Immigrant Status Indicator Technology (US-VISIT)'s Arrival Departure Information System (ADIS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf
  - SORN: http://edocket.access.gpo.gov/2007/E7-16473.htm

- USCIS's Central Index System (CIS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf
  - SORN: http://edocket.access.gpo.gov/2007/E7-375.htm

- USCIS's Computer-Linked Application Information Management System Version 3 (CLAIMS 3)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf
  - SORN: http://edocket.access.gpo.gov/2008/E8-22802.htm

- USCIS's Computer-Linked Application Information Management System Version 4.0 (CLAIMS 4)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims4.pdf
  - SORN: http://edocket.access.gpo.gov/2008/E8-22802.htm

- USCBP's Nonimmigrant Information System and Border Crossing Information
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_borderops.pdf
  - SORN: http://edocket.access.gpo.gov/2008/E8-17123.htm

- Department of State (DOS)'s Consular Consolidated Database (DOS-CCD)
  - PIA: http://www.state.gov/documents/organization/93772.pdf
  - SORNs:
    1) http://www.state.gov/documents/organization/102787.pdf
    2) http://www.state.gov/documents/organization/102790.pdf
    3) http://www.state.gov/documents/organization/102815.pdf

- ICE's ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf
  - SORN: http://edocket.access.gpo.gov/2010/2010-4099.htm

- USCIS's Enterprise Document Management System (EDMS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_iddmp.pdf
  - SORN: http://edocket.access.gpo.gov/2007/E7-375.htm

- Department of Justice's Executive Office of Immigration Review System (EOIR)
  - PIA: http://www.justice.gov/opcl/eoir_pia.pdf
  - SORN: http://edocket.access.gpo.gov/2004/04-10564.htm

- USCIS's Image Storage and Retrieval System (ISRS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf
  - SORN: http://edocket.access.gpo.gov/2007/07-1643.htm

- USCIS's Marriage Fraud Amendment System (MFAS)
  - SORN: http://edocket.access.gpo.gov/2007/E7-375.htm

- USCIS's Microfilm Digitization Application System (MiDAS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_midas.pdf
  - SORN: http://edocket.access.gpo.gov/2007/E7-375.htm

- USCIS's National File Tracking System (NFTS)
  - PIA: Referenced in: 1) PIA titled: USCIS Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS National Security and Records Verification Directorate/Verification Division http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_pcq_nsrv_update.pdf and 2) Application Connection and Information Sharing Agreement between USCIS Enterprise Service Bus (ESB) and USCIS NFTS System Owner

- USCIS's Refugees, Asylum, and Parole System (RAPS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_rapsapss.pdf
  - SORN: http://edocket.access.gpo.gov/2010/E9-31267.htm

- USCIS's Reengineered Naturalization Applications Casework System (RNACS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_rnacs.pdf
  - SORN: http://edocket.access.gpo.gov/2008/E8-22802.htm

- Immigration and Customs Enforcement (ICE)'s Student and Exchange Visitor Identification System (SEVIS)
  - PIA: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf
  - SORN: http://edocket.access.gpo.gov/2010/E9-31268.htm