Privacy Impact Assessment
for the

Verification Information System

Supporting Verification Programs

April 1, 2007

Contact Point
Elizabeth Gaffin
Privacy Officer
United States Citizenship and Immigration Services
202-272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

U.S. Citizenship and Immigration Services (USCIS) provides immigration status verification for benefits determinations and employment authorization through the Verification Division of USCIS. Presently, two programs exist to implement this mandate: the Systematic Alien Verification for Entitlements (SAVE) program for government benefits and the Employment Eligibility Verification/Basic Pilot Program for private employer verification of employment authorization for all newly hired employees. The Verification Information System (VIS), a composite information system incorporating data from various Department of Homeland Security databases, is the underlying information technology that supports these programs. USCIS is conducting this Privacy Impact Assessment (PIA) to describe updates to VIS that will improve the ability of USCIS to provide citizenship and immigration status information to users of SAVE and Basic Pilot.

Introduction

Congress in various statutes mandated that USCIS provide a system that verifies citizenship and immigration status of individuals seeking government benefits and whether a newly hired employee is authorized to work in the United States. USCIS implemented this mandate through the Systematic Alien Verification for Entitlements (SAVE) program for government benefits and the Basic Pilot Program for determining whether a newly hired employee is authorized to work in the United States.

The Verification Information System (VIS) is the technical infrastructure that enables USCIS to operate SAVE and Basic Pilot. VIS is a nationally accessible database of selected immigration status information containing in excess of 100 million records. Government agencies use SAVE information to help determine whether a non-citizen is eligible for any public benefit, license, or credential based on citizenship and immigration status. Private employers and government users use Basic Pilot information to determine whether a newly hired employee is authorized to work in the United States.

VIS is comprised of citizenship, immigration, and employment status information from several DHS System of Records, including Custom's and Border Protections' the Treasury Enforcement Communication Systems (TECS) (66 FR 52984), Image Storage and Retrieval System (ISRS) (66 FR 6672), USCIS's Central Index System (CIS) (72 FR 1755), and USCIS's Computer Linked Application Information Management System (CLAIMS 3) (64 FR 18052).

SAVE Program

The SAVE Program provides government agencies with citizenship and immigration information so that agencies can determine an individual's eligibility for government benefits. Government agencies input biographic information into VIS and if VIS has a record pertaining to the individual, the government agency will receive limited biographic information on the citizenship and immigration status of the individual applying for a benefit. If VIS does not have a record pertaining to the individual, VIS automatically notifies a USCIS Immigration Status Verifier (ISV). The ISV then conducts a manual search of other DHS databases to determine whether there is any other information pertaining to that individual that would provide citizenship and immigration status. If the ISV finds additional information,

citizenship and immigration status is provided to the requesting governmental user through VIS. The ISV will also update the appropriate record in USCIS' CIS database.

The REAL ID Act requires that beginning May 2008, with a possible extension until December 2009, all states routinely utilize USCIS's SAVE program to verify the legal status of applicants for drivers licenses and identification cards. This date may be postponed until December 2009 pursuant to a notice of proposed rule making. Currently, it is anticipated that states will use SAVE in the same manner as described throughout this PIA. If an update to VIS is required to accommodate REAL ID, this PIA will be updated to reflect those changes.

Basic Pilot

VIS also supports the Basic Pilot Program, a free and voluntary program for employers, that allows participating employers to verify the the employment eligibility of newly hired employees. The program is a collaboration between the Social Security Administration (SSA) and USCIS.

After an individual is hired by the employer and completes the Form I-9, Employment Eligibility Verification Form,[1] , employers input information from Sections 1 and 2 of the Form I-9 into the Basic Pilot portion of VIS. The query is first sent from VIS to SSA to verify social security information. If SSA cannot verify the employee's social security information, SSA will send a response to VIS that in turn will notify the employer of SSA's inability to verify the information provided by the employee. The employer is then required to provide information to the employee about how the employee may contact SSA to resolve any issues. If SSA is able to verify the employee's social security information and the individual is a U.S. Citizen (USC), a verification notification is provided to the employer. No further action is taken by VIS. If SSA is able to verify the employee's social security information and the individual is a non-USC, the VIS system continues the process in order to verify employment eligibility. Through VIS, USCIS provides the employer with a case verification number and the disposition of whether an employee is authorized to work in the United States. If VIS does not have a record pertaining to the individual, VIS automatically notifies an ISV. The ISV then conducts a manual search of other DHS databases to determine whether there is any other information pertaining to that individual that would provide employment eligibility status. If the ISV cannot determine the person's work eligibility, VIS notifies the employer that the employee must contact USCIS. If it is determined that an employee is not authorized to work after the employee is referred to SSA or USCIS, the employer may terminate the individual's employment. If the ISV finds additional information, updated employment eligibility is provided to the employer through VIS. The ISV will also update the USCIS record, contained in CIS, with the additional information found.

[1] All U.S. employers are responsible for the completion and retention of Form I-9 for each individual they hire for employment in the United States. This includes citizens and non-citizens. On the form, the employer must verify the employment eligibility and identity documents presented by the employee and record the document information on the Form I-9. Acceptable documents are listed on the back of the form, and detailed below under "Special Instructions."

Performing a verification query through the Basic Pilot system is only legally permissible after an offer of employment has been extended to an employee. The verification must be initiated no later than three days after the employee begins working. Information from the Basic Pilot cannot be used to pre-screen individuals, re-screen individuals after being employed for longer than three days, or discriminate against individuals legally authorized to work in the United States.

Updates to VIS

The purpose of this PIA is to provide information about these two programs, the underlying information technology supporting these programs, and updates to the programs that will improve the ability of USCIS to provide appropriate citizenship and immigration status information to users.

VIS is consolidating data elements from additional DHS Systems of Records in order to improve data completeness within VIS. USCIS is currently enhancing the employment verification function of VIS to allow an employer to query the system by inputting the new hire's USCIS receipt number, which is located on the secure Form I-551 (Permanent Resident Card) or the secure Form I-766 (Employment Authorization Document). The receipt number is a unique number associated with the issuance of the card. In addition, USCIS is piloting a new functionality that allows employers using Basic Pilot to compare the photographgraph contained on secure issued USCIS cards against the photograph on file in ISRS and/or BSS. These enhancements will significantly improve the speed at which USCIS will be able to verify the employment eligibility of many non-citizen new hires and reduce the likelihood of identity fraud through forged documents.

Once deployed, additional data elements will be included in the VIS system from the Biometric Storage System (BSS) and ICE's Student and Exchange Visitor Information System (SEVIS). In order to support programmatic goals, the system will have improved audit and reporting capability so that USCIS can better identify misuse of the system and programs supported by the system.

The above noted enhancements will significantly improve the speed at which USCIS will be able to verify the employment eligibility of many non-citizen new hires and reduce the likelihood of identity fraud through forged documents. As new functionality is introduced into VIS and the SAVE Program and Basic Pilot Program, this PIA will be updated.

Additionally, VIS will be the underlying technology for the implementation of the REAL ID Act for which a Notice of Proposed Rulemaking is being conducted. This PIA will be updated to reflect any changes needed to support the implementation of the Final Rule.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

Information Downloaded to VIS Database

Information contained in VIS is derived from other DHS systems. VIS receives daily downloads of relevant subsets of information about individuals who have come before USCIS pursuant to the Immigration and Naturalization Act, to include applications for immigration benefits, petitioners, and non-immigrant visa holders. Information contained within VIS may include citizenship and immigrant and employment information maintained by USCIS and non-immigrant information maintained by Customs and Border Protection (CBP). Specific information received in these downloads includes the following:

Data originating from USCIS's Central Index System (CIS). The CIS download includes data received from the Employment Authorization Document System (EADS).

About the Individual who comes before USCIS

- Alien Registration Number (A-Number)
- Name (last, first, middle)
- Date of birth
- Date entered United States (entry date)
- Country of birth
- Alien Status Code (Class of Admission)
- File Control Office code
- Social Security Number
- Admission Number (I-94 Number)
- Provision of Law code cited for employment authorization
- Office Code where the authorization was granted
- Date employment authorization decision issued
- Date employment authorization may begin (start date)
- Date employment authorization expires (expiration date)
- Date employment authorization denied (denial date)

Data originating from CBP's Treasury Enforcement Communications System (TECS)

About the Individual

- A-Number
- Name (last, first)

- Date alien's status was changed (status change date)
- Date of birth
- Class of Admission Code
- Date admitted until
- Country of citizenship
- Port of entry
- Date entered United States (arrival date)
- Departure date
- I-94 Number
- Visa Number

Data originating from USCIS's Image Storage and Retrieval System and/or Biometric Storage System (when deployed)

- Receipt Number
- A-number
- Name (last, first, middle)
- 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

Data originating from USCIS's CLAIMS 3

- Receipt number
- A-number
- Name (last, first, middle)
- Date of Birth
- Country of Birth
- Class of Admission
- I-94 number
- Date of Entry
- Valid To Date

Data originating from ICE' SEVIS

- Student and Exchange Visitor Identification Number (SEVIS ID)
- Name (last, first, middle)
- Date of Birth
- Country of Birth
- Class of Admission
- I-94 number
- Date of Entry

- Valid To Date

Data originating from Social Security Administration (SSA)

- Confirmation of employment eligibility based on SSA records or
- Tentative non-confirmation of employment eligibility and the underlying justification for this decision and
- Final non-confirmation of employment eligibility.

Immigration Status Information Collected from the Agency Using SAVE

Information collected from the Benefit Issuing Agency to facilitate immigration status verification may include the following:

About the Individual (e.g., applicant, employee)

- Receipt Number
- A-Number
- Name (last, first, middle initial)
- I-94 Number
- Date of birth
- User Case Number
- DHS document type
- DHS document expiration date
- SEVIS ID
- Visa Number

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

- Name of Agency
- Address
- Point of Contact
- Contact telephone number
- Fax number
- E-mail address
- Type of benefit for which the applicant has applied

About the Individual Agency User

- Name (last, first, middle initial)
- Phone Number
- Fax Number
- E-mail address

- User ID for users within the Agency

VIS-provided information, as a result of the verification process under SAVE

- Case Verification Number
- Entire record in VIS database as outlined above, including all information from CIS, SEVIS, TECS, and CLAIMS 3 and with the exception of the biometric information (photograph) from ISRS and/or BSS, once deployed.
- Immigration status (e.g. Lawful Permanent Resident)

Employment Authorization Information Collected from the Employer User Using Basic Pilot

Information collected in VIS to facilitate employment eligibility verification may include the following:

About the Individual (e.g., newly hired employee)

- Receipt Number
- Name (last, first, middle initial, maiden)
- A-Number
- Visa Number
- I-94 Number
- Social Security Number
- Date of birth
- Date of hire
- Claimed citizenship status
- Type of document used for Acceptable Form I-9 verification
- Acceptable Form I-9 Document expiration date

About the Employer

- Company name
- Street Address (Post Office Boxes are not acceptable)
- Employer Identificatioon Number
- North American Industry Classification System code
- Number of employees
- Number of sites
- Parent company or Corporate company
- Name of Contact
- Phone Number
- Fax Number

- E-Mail Address

About the Individual Employer User (e.g., Users at the Employers)

- Name (last, first, middle initial)
- Phone Number
- Fax Number
- E-mail address
- User ID

As a result of the verification process for Basic Pilot, the system will contain the following two types of information: Information provided by VIS and information provided by the employer relating to an employee who has undergone the verification process.

- VIS response
  - Employment authorized,
  - Case verification number,
  - Digital Photographgraph of newly hired employee who have been issued USCIS documents, and
  - VIS response
    - Tentative non-confirmation
    - Case in continuance
    - Final non-confirmation
    - Employment unauthorized or
    - DHS No Show.
- Disposition data from the employer
  - Resolved Unauthorized/Terminated
  - Self Terminated
  - Invalid Query
  - Employee not terminated
  - Resolved Authorized
  - Request additional verification, which includes why additional verification is requested by the employer user.

1.2 From whom is information collected?

From DHS Databases

VIS receives information from the following systems: CIS, SEVIS, TECS, CLAIMS 3, and ISRS and/or BSS (once deployed). Generally information from CIS, SEVIS, CLAIMS3, and ISRS/BSS is derived from applications/petitions submitted to DHS in which the subject is seeking an immigration benefit. The SEVIS system also contains information obtained from institutions of higher learning

(universities and colleges) to which individuals have applied for admissions. Information contained in TECS is obtained by DHS from documents presented by individuals entering or exiting the country.

From the VIS users about the Individual Applicant Requesting Benefits or Seeking Employment

VIS receives information about individual applicants requesting benefits from the benefit-granting agency or from participating employers requesting employment eligibility information about newly hired employees. The subject of the inquiries does not have direct access to VIS; rather, information concerning the individual is entered by an agent user of VIS (e.g., by a government Agency User or by an Employer User).

From the Agency (e.g., federal, state, local or other government agencies)

Agencies that participate in the SAVE program will collect information about individuals requesting a benefit, and will provide that information to the VIS application. The VIS database will also include information about the agencies using the system to determine eligibility of individual benefits.

From the Employer

Employers that participate in the Employment Eligibility Verification/Employment Eligibility Verification/Basic Pilot Program provide information about their respective company to the VIS application.

From the Agency/Employer User

Information is collected from the individual users of VIS (e.g., from Government Agency employees, their contractors and/or Employers).

1.3 Why is the information being collected?

Information is collected from the inquiring Agency to enable it to assess the eligibility of the applicant who has applied for benefits or licenses or from an employer in order to verify the employment eligibility of newly hired employees. Personally identifiable information from individual users of the system is collected in order to provide accountability of system usage in the event a problem arises with misuse of the system.

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

Immigration Reform and Control Act of 1986 (IRCA), P.L. 99-603, dated November 6, 1986

IRCA required the creation of a system for verifying the immigration status of non-citizen applicants for, and recipients of, certain types of federally funded benefits, and to make the system available to federal, state, and local benefit issuing agencies and institutions that administer such benefits.

Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), P.L. 104-193, 110 Stat. 2168, dated August 22, 1996

PRWORA required the establishment of regulations and interim guidance for the verification of immigration status of persons applying for "Federal public benefits."

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208, dated September 30, 1996

The IIRIRA required a means to respond to inquiries by federal, state, and local benefit issuing agencies and institutions seeking to verify or determine the citizenship or immigration status of any individual within the jurisdiction of the Agency for any lawful purpose. The SAVE Program's automated and manual verification processes provide federal, state, and local benefit issuing agencies and institutions with information which will assist them in determining an individual's eligibility. Title IV of the Act requires the establishment of a Basic Pilot Program with voluntary participation by Employers who could use this system to determine whether newly hired employees were authorized to work in the United States.

Basic Pilot Program Extension and Expansion Act of 2003 (Pub. Law 108-156), dated November 19, 2003

This Act extends the Basic Pilot to November 2008.

The REAL ID Act of 2005 (REAL ID), Division B of Public Law 109-13, dated May 11, 2005

REAL ID established certain minimum standards for the issuance of state-issued driver's licenses and state-issued identification cards in order for those documents to be acceptable for Federal purposes. To meet the requirements of the REAL ID Act, by May 11, 2008, states must, among other things, verify the lawful status of every driver's license and identification card applicant. The Act also mandates that all States enter into a Memorandum of Understanding (MOU) with the SAVE Program by September 11, 2005 and requires that states be in full compliance with the Act by May 2008, in order to have their state-issued driver's licenses and state-issued identification cards recognized by the Federal government for official purposes. This date may be postponed until December 2009 pursuant to a notice of proposed rule making. One provision is the routine verification of lawful status through the SAVE Program of all non-citizen applicants for a driver's license or state-issued identification card.

1.5 How is the information collected?

An agency seeking to establish citizenship or immigration status or the employer seeking employment eligibility status about the individuals, may do so by inputting information through secure means to include: 1) Secure File Transfer Protocols for batch transfers, 2) dial up systems which are currently being phased out, 3) secure USCIS web site, or 4) web services that allow direct connection between USCIS and the employer.

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

Privacy Risk: Collection of extraneous information

Mitigation: The VIS database contains only those data elements needed to accomplish the searches required by the SAVE and/or Basic Pilot program. VIS collects a minimum set of personally identifiable information about the subject (benefit applicant or employee) to obtain his/her immigration status from the data contained within the VIS database. VIS collects a minimum set of personally identifiable information from the system user to enable proper operation and administration of the system and to provide answers to queries.

Privacy Risk: Inaccurate information attributed to the individual

Mitigation: VIS is being updated to include data enhancements and downloads from additional DHS systems in order to improve the completeness of data within VIS. Additionally, if VIS is unable to verify an individual's status in order to obtain a benefit or employment authorization, an ISV will review the information and will conduct searches of other DHS databases in order provide further verification so that an individual's status can be confirmed. Updated information that arises from this process will be added to VIS and to USCIS CIS database to ensure the discrepancy is rectified.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

VIS is used to a) to assist a federal, state, or local governmental entity in determining an individual's eligibility for benefits or licenses, based on immigration status, and b) to determine whether a newly hired employee is authorized to work in this country based on the existence of a valid social security number and lawful immigration status. USCIS has signed Memorandum of Understandings (MOUs) with all Agencies and employers that use VIS for SAVE or Basic Pilot. The MOU outlines proper use of the system.

With the new enhancements to VIS, Basic Pilot will provide employers access to digital photographgraphs from ISRS and BSS, when deployed, in order to assist the employer with another means of verifying an employee's identity. These images will be stored within VIS. If there appears to be evidence of document fraud, the employer is instructed to notify USCIS.

The REAL ID Act requires that beginning May 2008 with a possible extension for States until December 2009, all states must routinely utilize the SAVE program to verify the lawful presence status of drivers license and identification card applicants in order for those documents to be acceptable for federal uses. This date may be postponed until December 2009 pursuant to a notice of proposed rule making. If changes are required to VIS in order to support the implementation of the Final Rule associated with the Act, this PIA will be updated.

Additionally, the information used and retained in the system may be used for the following purposes: 1) On a case by case basis to ICE for fraud purposes, to aid it in worksite investigations to include incidences of as with multiple uses of the same SSN, same A-Number, same I-94 Number, etc); 2) Program analysis; 3) Compliance monitoring (e.g., to ensure users are following procedure).

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

With enhancements to VIS, the system will have improved audit and reporting capability to better assist USCIS in identifying misuse of the system. In particular, USCIS will focus on whether the system is being used in a discriminatory fashion, i.e., used to verify some employees but not others as well as whether the system is used to prescreen employees as opposed to after an offer of employment has been extended.

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

Information contained within the VIS database is derived from other systems. Data contained within the VIS database is downloaded from CIS, SEVIS, TECS, CLAIMS 3, and ISRS and/or BSS, once deployed.

VIS is consolidating the data from additional DHS System of Records to improve data completeness in order to, reduce the number of additional verifications required by ISV. The improvements to be made to the system include:

- Downloading data from ICE's Student and Exchange Visitor Information System (SEVIS).
- Downloading data from CBP's TECS, to include real time air and sea arrival data for aliens (real time land border arrival data is already obtained from the Form I-94 feeds).
- Using USCIS CLAIMS 3 data that would include change of status and extension of status information on non-citizens and non-immigrants. This data will be applied to the TECS extract, improving its quality.

In response to an initial verification query on an individual, VIS will provide the immigration status of that individual if stored in the database. If no record is found pertaining to the individual, then an ISV will perform a manual search of additional DHS systems to determine citizenship and immigration status and employment eligibility status.

In cases where the ISV identifies inaccurate information, two methods of correction can occur. First, the ISV enters immigration status and/or employment eligibility response data directly into VIS, which is then transmitted to the agency or employer through VIS. This occurs when the initial verification is inconclusive or when the agency and or employer user observes a discrepancy with names or documents, requiring the ISV to search other data sources to produce definitive results. If the ISV determines that the underlying USCIS database has inaccurate information, the ISV will either update or request an update to the underlying database to correct the record that will then be downloaded to the VIS database in the next nightly feed.

With respect to information collected from users, it is incumbent upon both the individual providing his or her information as well as the Agency User or Employer User performing the query to

verify the accuracy of information being provided to VIS about the individual. The Basic Pilot Program provides a confirmation page to the employer user to review prior to submitting the query.

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.

The information contained in VIS is used only to respond to inquiries from authorized agencies and/or employers. Agencies and employers must sign a Memorandum of Understanding (MOU) with DHS stating the intended use of the system and agreeing to the established security requirements. Each MOU contains provisions for training, policies, safeguarding of information obtained from the system, and procedures/instructions on the use of VIS.

For employment verifications, VIS has been modified to include a confirmation screen prior to submittal of an initial verification. This provides the Employer User with an opportunity to see the information entered and make corrections to that information prior to submittal.

Privacy Risk: Misuse of information

Mitigation: MOUs are established with outside entities to help ensure the proper use of the responses returned by VIS. The MOU outlines the appropriate use of information by end users. With enhancements to VIS, the system will now have improved audit and reporting capability so that USCIS can better identify misuse of the system. USCIS plans to increase enforcement actions in response to allegations of misuse.

Privacy Risk: Unauthorized Access to Information

Mitigation: The information contained in VIS is used only to respond to inquiries from authorized agencies and/or employers. Agencies and employers must sign an MOU with DHS stating the intended use of the system and agreeing to appropriate safeguards, use, maintenance, and disclosure of the data. Additionally, USCIS plans to increase enforcement of misuse of the system.

Privacy Risk: Inaccurate Information Attributed to an Individual

Mitigation: With the addition of information from SEVIS and BSS, when deployed, VIS will have more accurate information so that fewer individuals will require a manual search completed by an ISV. In addition, the ISV procedures for conducting manual searches and updating any underlying information contained within CIS improves the accuracy of the information in VIS overall.

Section 3.0
Retention

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

VIS-Generated Data

VIS generated data related to the verification process through SAVE includes: case verification number, citizenship and immigration status, and all records on file in VIS on an individual. VIS generated data related to the verification process through Basic Pilot includes: case verification Number, Digital Photographgraph on file, VIS response regarding employment status, and disposition data received from the employer. VIS currently follows the data retention and destruction policies as documented in NARA retention/disposition schedule N1-85-90-3, dated 4/24/90 In particular, "Completed verifications are archived to a storage disk monthly, and destroyed five (5) years after the last month contained on the disk."

NARA retention/disposition schedule N1-85-90-3, dated 4/24/90 indicates:

- Secondary Verification Manual Log – Destroy 5 years after the month displayed on the paper log
- Form G-845S, "Document Verification Request" – Destroy 5 years after the date status verification was completed
- Form G-845, "Document Verification Request" – Destroy 5 years after the date status verification was completed

USCIS will be submitting an amendment to the NARA schedule which will increase the time records are stored and retained in the VIS Repository for twenty (20) years, from the date of the completion of the verification. VIS will retain data contained within this system to facility USCIS' ability to conduct trend analysis that may reflect the commission of fraud or other illegal activity related to misuse of either the SAVE or Basic Pilot program and to facilitate the reconstruction of an individual's employment eligibility history. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits.

Information Downloaded to VIS Database

Data derived from other systems will be retained in accordance with data retention schedules specific to those systems.

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

NARA has approved retention/disposition schedule N1-85-90-3, dated 4/24/90. However, as discussed in Section 3.1 above, USCIS is seeking to amend its current retention schedule to extend this period for a total of 20 years.

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

Information retained in the system is retained for: 1) Fraud purposes, on a case by case basis to aid in ICE worksite investigations to include incidences of as with multiple uses of the same SSN, same A-Number, same I-94 Number, etc, 2) Program analysis; 3) Compliance monitoring (e.g., to ensure users are following procedure); and 4) To enable USCIS to reconstruct and individual's employment eligibility history.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

Presently, there are two DHS components that participate in the SAVE Program, the Transportation Security Administration (TSA) and the Federal Protective Service (FPS). Both TSA and FPS have signed MOUs to participate in the SAVE Program and access VIS. In addition to the contractors and employees in the SAVE Program and the ISVs located throughout the country, the primary users of VIS are the external government-benefit granting agencies and Employers. On a case-by-case basis, information is shared with law enforcement components within DHS conducting law enforcement investigations.

The USCIS Verification Division plans to establish an office to monitor employers' use of the Basic Pilot and promote compliance with correct program procedures. With updates to VIS, the system will now be able to provide improved reports to allow possible follow up with appropriate law enforcement entities in the event fraud and misuse appear to be occurring with the use of the system. The office is contemplating developing a Memorandum of Understanding with Immigration and Customs Enforcement (ICE) so that the program can forward possible enforcement leads in accordance with developed referral procedures. Information shared may include data obtained during USCIS's enhanced audit process.

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

See Section 4.1, above.

4.3 How is the information transmitted or disclosed?

DHS components that are SAVE users are provided information in the same manner as all other government SAVE users through a variety of means as described below. In accordance with appropriate security protocols, various access methods to VIS are offered to the user; information is transmitted by various means depending on the access method being used. A user may obtain access by submitting inquiries through the web/internet, by utilizing the batch access method, or by a web services method where program-to-program communication is established between a user organization's application program and VIS.

VIS provides the following access methods for internal DHS Users for SAVE:

- Web/Internet - There are several web access methods tailored to the needs of various types of government agencies. The web access methods allow users to establish a secure internet connection to VIS, submit queries, receive immediate responses based on the contents of the non-citizen status database, submit requests for manual additional verifications, and run reports.
- Agency Priority Batch - The batch access method is available to high-volume user organizations. The batch interface is non-interactive and involves the transmission of a file of requests to VIS and retrieval of a response file from VIS via Secure File Transfer Protocol over the Internet.
- Agency Web Services - This access method allows program-to-program communication between a user organization's application program and VIS using a secure protocol over the Internet. This allows the user organization's application program to submit verification requests and receive responses.
- Dial Up Services – This older method is used by individuals who have analogue telephones and modums and is not available to new users. Current users will be tranisitioned to another access method in the near future.

Basic Pilot is not used internally by DHS for verification purposes.

USCIS is developing a more robust auditing program. It may share information on a case by case basis with appropriate law enforcement entities, such as ICE. This information will be shared in accordance with appropriate security and privacy controls relating to personally identifiable information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Privacy Risk: Access to VIS by unauthorized individuals

Mitigation: Requests for access must be approved by a supervisor, after which the request is forwarded to the SAVE Program who approves the request and issues a password, or denies the request. DHS employees are also required to take and pass annual computer awareness training.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

Currently, there are 205 participating government agencies for SAVE and over 14,000 employers for Basic Pilot. Program participation is increasing monthly, as more government agencies and employers are registering to participate in the programs. Included below is a sampling of program participants:

- Social Security Administration
- Private Sector Employers with a signed MOU
- State Departments of Motor Vehicles
- Housing and Urban Development (HUD) project owners/housing authorities
- State Labor Agencies
- State Social Service Agencies
- U.S. Department of Education
- Mohegan Tribal Gaming Commission
- City of New York Human Resources Administration
- Palm Beach County Property Appraiser
- Transportation Security Administration
- Office of Personnel Management
- Federal Protective Service
- Department of Defense Manpower Data Center

In addition, USCIS may provide program related data with the Department of Justice (DOJ), Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or immigration discrimination.

5.2 What information is shared and for what purpose?

For SAVE users verifying information for benefits

Federal, state, and local government entities with the exception of HUD, query VIS by entering an A-Number or I-94 Number. In response, VIS provides the Agency user with the name (last, first, middle), date of birth, date of entry, country of birth, class of admission code, date admitted to, and, if applicable, Employment Authorization Document, (EAD) expiration date, the case verification number, and the disposition of citizenship or immigrant status. The citizenship or immigration status allows the agency to determine benefit eligibility of the applicant.

HUD includes users who are private entities and non-government users, such as projects owners, housing authorities, and landlords, who must verify the citizenship or immigration status of potential recipients of housing in order to fulfill government requirements. The HUD non-government users are required to provide A-Number or I-94, the individuals first and last name, date of birth, and the DHS document type issued to the individual. . This is the only group in the SAVE Program required to provide additional identifying information. The HUD user also receives somewhat abbreviated results from VIS which includes the first, last and middle name of the individual, the Class of Admission (COA), the Country of Birth, the Date of Entry, and the System Response

For Basic Pilot users verifying information for employment

Employers query VIS by providing information from Sections 1 and 2 of the Employment Eligibility Verification Form I-9. The query is initially sent through VIS to SSA to confirm employment authorization. If SSA cannot confirm the information provided, the individual is provided instructions, by his or her employer on how to contact the SSA for possible resolution. If the individual is an alien and, SSA is able to confirm the individual's name, date of birth and a SSN match can be made their records, the query continues with USCIS to verify employment authorization. The information shared by VIS with the Employer User includes the case verification number and the disposition of whether an employee is authorized to work.

5.3 How is the information transmitted or disclosed?

In accordance with appropriate security protocols, the various access methods to VIS are offered to the user; information is transmitted by various means depending on the access method being used. A user may obtain access by submitting inquiries by way of the web/internet by utilizing the batch access method or by a web services method where program-to-program communication is established between a user organization's application program and VIS.

VIS provides the following access methods SAVE users:

- Web/Internet - There are several web access methods tailored to the needs of various types of government agencies. The web access methods allow users to establish a secure Internet connection to VIS, submit queries, receive immediate responses based on the contents of the non-citizen status database, submit requests for manual additional verifications, and run reports.
- Agency Priority Batch - The batch access method is available to high-volume user organizations. The batch interface is non-interactive and involves the transmission of a file of requests to VIS and retrieval of a response file from VIS via Secure File Transfer Protocol over the Internet.
- Agency Web Services - This access method allows program-to-program communication between a user organization's application program and VIS using a secure protocol over the Internet. This allows the user organization's application program to submit verification requests and receive responses.

VIS provides the following access methods for Basic Pilot Users:

- Web Basic Pilot (Web-BP) - Web-BP is an Internet-based application that allows employers to verify the work authorization of ALL newly hired employees.
- Web Designated Agent Basic Pilot (Web-DABP) - Web-DABP contains the same functionality as Web-BP and also allows a designated agent to perform employment verification for one or more client companies.
- Employer Priority Batch - The batch access method is available to high-volume user organizations. It permits the transmission of a file of requests to VIS and retrieval of a response file from VIS via Secure File Transfer Protocol over the Internet.
- Employer Web Services - This access method allows program-to-program communication between a user organization's application program and VIS using a secure protocol over the Internet. This allows the user organization's application program to submit verification requests and receive responses.
- Dial Up Services – This older method is used by individuals who have analogue telephones and modums and is not available to new users. Current users will be transitioned to another access method in the near future.

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?

Separate MOUs exist for both the SAVE program for benefits determination and the Basic Pilot Program for employment authorization purposes.

Before an agency may use VIS to obtain immigration status information, an MOU must be signed between that agency and DHS/USCIS to establish the terms and conditions governing its participation in the SAVE Program. The MOU clearly states its purpose as verifying the citizenship and immigration status of alien applicants for benefits granted by the Agency. The MOU used for benefits restricts the Agency from disclosing any information to other than the applicant to whom it pertains. The MOU used for employment prohibits the Employer from disseminating any information to other than those employees needing it to perform the Employer's responsibilities under the MOU.

Before an employer may use VIS to obtain employment authorization information, an MOU must be signed between that employer, the Social Security Administration (SSA), and DHS/USCIS to set forth the points of agreement regarding its participation in the Basic Pilot. The MOU clearly states its purpose as confirming employment eligibility of all newly hired employees. It also memorializes an employer's agreement to safeguard the information it receives to ensure the privacy of the subject of the search.

Memorandum of Understanding – SAVE for Citizenship and Immigration Status:

Before an agency may use VIS to obtain immigration status information, an MOU must be signed between that agency and USCIS to establish the terms and conditions governing its participation in the SAVE Program.

The REAL ID Act of 2005 (REAL ID), Division B of Public Law 109-13, dated May 11, 2005 for SAVE Citizenship and Immigration Status:

As required by the REAL ID Act of 2005, all states and four territories were required to enter into a Memorandum of Understanding (MOU) with the SAVE Program by September 11, 2005. Currently, there are only four states that have not entered into a MOU with the DHS. The program is currently evaluating the possible need for a subsequent Memorandum of Agreement (MOA) as part of implementation of the requirements of the Act prior to May 2008.

Memorandum of Understanding – for Basic Pilot Employment Status:

Before an employer may use VIS to obtain employment authorization information, an MOU must be signed between that employer, the Social Security Administration (SSA), and USCIS to set forth the points of agreement regarding its participation in the USCIS's Basic Pilot Program. Prior to receiving access to the system, every user must first take a tutorial instructing participants on the proper use of the system as well as the proper handling of any information obtained from the system and must successfully pass a mastery test.

5.5 How is the shared information secured by the recipient?

The SAVE MOU used for benefits, including for the issuance of a driver's license, requires the agency to comply with the Privacy Act and other applicable law in the safeguarding, maintaining, and disclosing of any data received. The agency does not download the information from VIS, but rather is able to go back to VIS and search past verifications.

The Basic Pilot MOU used for employment requires the employer to safeguard the information it receives from SSA and DHS, and to ensure that it is not used for any other purpose other than as provided in the MOU. In addition, the employer must acknowledge that the information it receives from SSA is governed by the Privacy Act (5 USC Section 552a) as well as the Social Security Act (42 USC Section 1306A) and that "any person who obtains this information under false pretenses or uses it for any purpose other than as provided in this MOU may be subject to criminal penalties".

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

There are separate on-line tutorials and mastery tests for benefits and employment. Both tutorials cover processes and procedures for the appropriate use of the system. Only employers are required to complete the tutorial and pass the mastery test.

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

Privacy Risk: Unauthorized Database Searches

Mitigation: Non-government agency users and employer users must provide multiple pieces of biographic information about a subject before a search will be allowed by VIS (e.g., A-Number plus name, date of birth, etc). A system change is under development that would apply this restriction to all user types within VIS. The USCIS Verification Division plans to establish an office to monitor employers' use of the Basic Pilot and promote compliance with correct program procedures. This office will compile reports analyzing various areas in which the Basic Pilot program can be misused. This office will review options by which to monitor authorized database searches.

Privacy Risk: Improper use

Mitigation: Information obtained from VIS is limited and responsive only to information provided by the user. MOUs are established with all agencies and employers to help ensure the proper use of VIS. Online tutorials and manuals for the proper use of VIS and safeguarding of the information are available to all users. Employer users are required to complete the tutorial and pass the mastery test before system access is granted. Information obtained from VIS is also limited and responsive only to information provided by non-government agency users and employers. In addition the new audit reports will allow USCIS to identify possible misuse.

Privacy Risk: Distribution of information to unintended recipients

Mitigation: The terms and conditions of the MOUs require the user to safeguard the information and to ensure that it is not used for any other purpose other than as provided in the MOU.

Privacy Risk: Unintended Misuse of VIS Information

Mitigation: Online tutorials for the proper use of VIS and safeguarding of the information are offered to all users. Employer users are required to complete the tutorial and pass the mastery test before system access is granted.

Privacy Risk: Intentional misuse of VIS

Mitigation: In FY07, the USCIS Verification Division plans to establish an office to monitor employers' use of the Basic Pilot and promote compliance with correct program procedures.

Section 6.0
Notice

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

A Systems of Records Notice (SORN) will be published for VIS at the same time this PIA is published. The updated VIS SORN will cover the previously published for the Verification and Information System (VIS) Justice/INS-035 published October 17, 2002 (67 FR 64134) and Alien Status Verification Index (ASVI) Justice/INS-009 published September 7, 2001 (66 FR 174).

Form I-9 Employment Eligibility Verification

Once completed, this form provides the basis for Employers to verify the eligibility of individuals for employment through VIS. The DHS, OMB approved instruction form that accompanies the Form I-9 contains the following Privacy Act Notice:

> **Privacy Act Notice.** The authority for collecting this information is the Immigration Reform and Control Act of 1986, pub. L. 99-603 (8 USC 1324a)
>
> This information is for employers to verify the eligibility of individuals for employment to preclude the unlawful hiring, or recruiting or referring for a fee, of aliens who are not authorized to work in the United States.

MOUs

MOUs, used both for benefits and employment, impose compliance with the Privacy Act. The MOU used for employment also requires that Employers display a poster that is clearly visible to prospective employees which indicates that it is participating in the Basic Pilot Program established by DHS and SSA to aid Employers in verifying the employment eligibility of all newly hired employees.

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

Benefits issuing and licensing agencies require applicants to provide the information relating to their citizenship and immigration status in order to process their applications for benefits/licenses. The MOU used for benefit-issuing and licensing agencies requires the agency to obtain a written release from each applicant authorizing the release of DHS information to the agency. In the absence of information

being provided by the applicant, citizenship and immigration status cannot be provided and individuals would not be eligible to receive the benefit for which they were applying.

Employer participation in the Basic Pilot is voluntary for employers, but if an employer chooses to participate all newly hired employees must be subject to the screening. For those participating Employers, the penalty to an employee who chooses not to provide information may be termination from his/her job.

As previously stated, the MOU used for employment purposes requires that employers display a poster that is clearly visible to prospective employers, which indicates that it is participating in the Basic Pilot Program established by DHS and SSA to aid employers in verifying the employment eligibility of all newly hired employees. Continued employment is contingent upon the employee participating. If the initial verification is not confirmable, the employee is given the opportunity to contest. If the employee contests, the MOU requires the Employer to provide the employee with notice of how to contact the SSA and/or DHS to resolve.

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?

Individuals who are screened through the SAVE program or the Basic Pilot program are either requesting a benefit or are working for an employer who is participating in the Basic Pilot Program. An individual's information is used solely to query the VIS database to ascertain whether or not an individual is in a lawful immigration status and/ or whether he or she is employment authorized. The employee is given clear notice at the time of employment that an employer is participating in the Basic Pilot Program. Failure to provide consent may result in a determination of ineligilbilty for a particular benefit or the termination of employment.

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

Privacy Risk: Insufficient notice of the collection and use of the information by the Agency Users.

Mitigation: Applicants are given notice through the publication of System of Records Notices, and in the case of employment verifications, a Privacy Act Notice on the instruction form that accompanies the Form I-9. An employer in the Basic Pilot Program must display a poster that is clearly visible to prospective employees which indicates that it is participating in the Basic Pilot Program established by DHS and SSA to aid employers in verifying the employment eligibility of all newly hired employees. Once an employer signs on to be a participant in the Program, only newly hired employees' employment eligibility statuses may be checked. For newly hired employees, continued employment is contingent upon the employee participating. If the initial verification is not confirmable, the employee is given the opportunity to contest. If the employee receives an SSA or DHS Tentative Non Confirmation

or, the MOU requires that the employer provide the employee with notice of how to contact the SSA and/or DHS to resolve outstanding issues associated with the tentative Non Confirmation.

This mitigates the risk that benefit applicants and or newly hired employees who otherwise would not be informed of what information is being used, how it is being used, who is using it and the mechanisms in place to protect the privacy of their information.

Section 7.0
Individual Access, Redress and Correction

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

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

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 erroneous information?

If an employee receives a "tentative non-confirmation" from DHS USCIS, the employer must provide a letter to the employee informing him/her of his/her rights to contest the "tentative non-confirmation." If an employee decides to contest a "tentative non-confirmation" from the initial verification query, the Employer must abide by the MOU by providing notice to the employee of their "tentative non-confirmation status" and allow the employee 10 days to resolve any discrepancies. This process is described in more detail in the Basic Pilot User Manual and Web-Based Tutorial, both of which are required readings for all users.

In general, individuals should direct all requests to contest or amend their information contained in the VIS database, with appropriate proof of identity, class of admission, and other relevant identifying 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 (e.g., CIS, EADS) or referred to the appropriate agency (e.g., CBP for TECS). If the source of data is from a USCIS download (i.e., CIS) and

USCIS confirms the data is in error, USCIS will modify the data in the original database (e.g., CIS or EADS).

Alternatively, the individual may appear in person, with accompanying supporting documentation, including proof of identity, class of admission, and other relevant identifying information if necessary, at a District Office and request that the Immigration Information Officer to effect the change.

VIS agency and employer users may change their profile information directly within the VIS application.

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

When an employee contests a "tentative non-confirmation," the employer provides both a written Referral Notice and a Contest Notice to the employee, providing information on how to contact SSA or DHS, as appropriate.

The individual applying for benefits may be notified by the benefit-bestowing Agency on the process for correcting their information with DHS.

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.

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

Privacy Risk: Individuals will not gain access to their personally identifiable information

Mitigation: Individuals are provided the opportunity to access their own information through the FOIA/PA process. There is a specific redress process previously defined for individuals that receive tentative non-confirmations. Employers must provide the documentation mentioned in Section 7.3. This enables individuals to ascertain what personally identifiable information has been collected about them and to determine whether any of the data is erroneous. Thereafter, an individual may seek to have the erroneous information corrected by submitting a Privacy Act request. During the redress process defined in Section 7.3, information can be corrected in the SSA database or through Immigration Status Verifiers for erroneous information contained within DHS systems.

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.)

Individuals who are the subjects of verifications do not have access to VIS directly.

Benefits, SAVE Program

VIS allows two types of external users to submit queries against the VIS database: "trusted users" (i.e., government Agency Users), and other "non-trusted users" (i.e., non-government Agency Users whose accounts are administered by government agencies such as Housing and Urban Development Project Owners/ Housing Authority).

VIS is only accessible internally by USCIS, for example, by the ISVs. All access to the internal VIS module of VIS requires passwords issued by the DHS Password Issuance and Control System (PICS) office in accordance with the policies of that office and DHS guidance.

Employment, Basic Pilot Program

VIS allows the following types of authorized Employer Users to submit queries against the VIS database:

Corporate Administrator: This user type can view reports for all companies associated with the corporate account. They can also update their personal user profiles and the profiles of other users throughout different company sites associated with the corporate account. This user can also register new locations and users, terminate access for existing locations, and perform site and user maintenance activities for all sites and users associated with the corporate account.

General User: This user type performs verification queries, views reports, and has the capability to update their personal user profile.

Program Administrator: This user type is responsible for creating user accounts at their site for other Program Administrators and General Users. They have the responsibility to view reports, perform queries, update account information, and unlock user accounts.

VIS is only accessible internally by USCIS, for example by ISVs. All access to the VIS module of VIS requires passwords issued by the DHS Password Issuance and Control System (PICS) office in accordance with the policies of that office and DHS guidance.

8.2 Will contractors to DHS have access to the system?

VIS, including all the equipment and communication links, is housed in a Contractor-owned data Center. In general, the Contractor provides the SAVE Program with all of the support required to meet the following SAVE-identified objectives:

- Management and administration of VIS, its databases, and subsystems;
- Design and implementation of pilot capabilities in support of the SAVE Program mission;
- Integration of selected capabilities into the VIS that have been demonstrated and tested as pilots or otherwise approved by the SAVE Program;
- Operate and maintain VIS;
- Design and implement changes to VIS resulting from additional requirements stemming from future legislative decisions.

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

Yes.

Access to the external module of VIS is determined based on role, and includes verification privileges and administrative privileges.

Access to the internal module of VIS is also determined based on role. The user's level of access is dependent on the duties they perform. There is a Supervisor level that receives all the cases and distributes them to the General users. Supervisors are also allowed to perform user administration on the system (reset passwords, change user contact information), as well as modify server or database operations. General user access allows SVS users to respond to both manual and automated requests. An ISV user has the ability to review and, depending on permissions, possibly modify, personal data for non-citizens. Access is granted in such a way that there is minimal potential for damage or personal gain. Access to the VIS source code is protected so that fundamental changes to the application cannot be made by unauthorized individuals.

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

The SAVE Program administers access to VIS. The SAVE Program requires potential enrollees and users to register for participation in the SAVE Program and sign a Memorandum of Understanding. If the user is an Employer he or she must also sign an Employee Information Page if participating in the Employer Pilot program. Once the required documentation is submitted, all users are mandated to complete a web-based training course that explains functionality and security requirements.

Agency Access

VIS allows users to submit queries, receive immediate responses based on the contents of the non-citizen status database, submit requests for manual additional verifications, and run reports.

Agency access to VIS is managed by the following procedures:

- WEB-1 Access Method Reference for Verification Information System (VIS), dated September 1, 2005.
- WEB-2 Access Method Reference Customer Processing System (VIS 1.0), Version 1.0
- WEB-3 Access Method Reference for Verification Information System (VIS), dated September 1, 2005

Employer Access

If the employee claims to be either a U.S. citizen or a lawful permanent resident, VIS checks the employee's Social Security Number (SSN) against the SSA database. For a lawful permanent resident, VIS also checks the employee's Alien Number against the VIS database. For other non-citizens, VIS forwards the I-94 number and supporting information to an Immigration Status Verifier.

In all of these cases, VIS returns the case resolution to the user. VIS also enables an Employer to create reports, manage user accounts, and perform password resets.

Employer access to VIS is described in the Basic Pilot User Manual.

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

When a new MOU is signed either for the Basic Pilot Program or SAVE, roles and responsibilities are assigned and approved by the USCIS supervisor. The VIS Helpdesk periodically reviews user lists and disables inactive accounts where necessary and on an interim basis.

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

VIS has a comprehensive audit trail tracking and maintenance function that stores information on who submits the query, when the query was run, what the response was, who receives the response, and when the response was received. The VIS Helpdesk periodically reviews user lists and disables inactive accounts where necessary. Each Agency signs a Memorandum of Understanding with DHS defining the use of VIS, the handling of account information, and security compliance requirements. Failure to comply with security policies can result in loss of access to VIS, at the discretion of DHS.

As stated in Section 2.2, the USCIS Verification Division plans to establish an office to monitor employers' use of the Basic Pilot and promote compliance with correct program procedures.

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

Internal users of VIS take the mandatory, annual DHS Information Technology security awareness training.

External users of VIS are provided an on-line tutorial that explains the SAVE Program or Basic Pilot Program, as appropriate. The tutorial also covers the procedures associated with the use of VIS, The tutorial does not specifically provide any Privacy training, but will be updated to include this information.

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

Yes. VIS received a Full Certification and Accreditation (C&A) in April 21 2005 (expiration is April 21, 2008).

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

Privacy Risk: Unauthorized access to information

Mitigation: Access to VIS is limited to authorized users. Employer users must take program-specific training, pass a mastery test, and possess valid IDs and passwords. Benefits users take program-specific training and are granted system IDs and passwords based upon their mission requirements.

Privacy Risk: VIS data being altered by external users of the system

Mitigation: All VIS external user access shall be "read-only." The USCIS through its contractor, Computer Sciences Corporation and the USCIS Monitoring office will monitor access to the database by the designated users to identify any unusual activity or access.

Privacy Risk: Non-authorized users may have indirect access to personal information

Mitigation: Idle accounts shall be logged-off after a period of inactivity.

Privacy Risk: VIS data being tampered with by the contractor

Mitigation: The contractor shall protect the VIS data and all support data files from unauthorized access or tampering.

Privacy Risk: Access by unauthorized agent user

Mitigation: An MOU must be signed by the agent user, SSA if for employment authorization, and DHS/USCIS prior to access being granted. Additionally, data is only provided back to the originator

or designee of the requesting Agency. Data from VIS is directly connect to any other IT system and is not shared with any other system.

Section 9.0 Technology

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

VIS was built from the ground up, and is a consolidated application composed of two main application subcomponents: the Customer Processing System (VIS), and the Status Verification System (SVS). VIS replaced the Alien Status Verification Information (ASVI) System. VIS is a transfer of the ASVI functionality from a legacy mainframe platform to a modern system comprised of Windows 2000 Intel servers and AiX UNIX servers. The SVS subcomponent is the integration of the previously independent Case Management System (CMS) into the consolidated VIS.

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

Benefits granting agencies are considered "Trusted Users" and are treated differently from "Non-Trusted Users" (non-government users) in that non-government users must provide additional information about the subject before VIS will allow a query to be performed.

VIS has been determined to have a sensitivity level of 2 in accordance with DHS Security Directive 4300A. Technical controls have been put in place commensurate with this level to include the requirement of password to obtain VIS access. VIS has an automated mechanism to ensure that users change their passwords at a specified interval. User IDs are locked after several failed attempts to logon to VIS. Also, VIS provides protection against password re-use. Additionally, inactive VIS sessions will timeout, requiring the user to log in.

The VIS database includes extensive audit trail capabilities for all user account and query activity. For each functional transaction, the transaction start time, end time, user ID that initiated the transaction, and the access method used are recorded. All audit logs have restricted access based on user roles included in the VIS application. These logs are external to system administration access methods and are reviewed by the Contractor's ISSO.

9.3 What design choices were made to enhance privacy?

As discussed in previous sections:

- The VIS database contains only those data elements needed to accommodate the searches intended by the SAVE program.

- For employment verifications, VIS has been modified to include a confirmation screen prior to submittal of an initial verification. This provides the Employer User with an opportunity to see the information entered and make corrections prior to submittal.
- Non-government agency users and Employer users must provide multiple pieces of biographic information about a subject before a search will be allowed by VIS (e.g., A-Number plus name, date of birth, etc). A system change is under development that would apply this restriction to all user types within VIS.
- Idle accounts shall be logged-off after a period of inactivity.

Additionally:

- All password data is encrypted within VIS.
- VIS is located within a multi-layered firewall architecture.
- All access to the internal module of VIS requires passwords issued by the DHS Password Issuance and Control System (PICS) office in accordance with the policies of that office and DHS guidance.
- VIS uses HTTPS protected communications during all data transmissions between the client workstation and the Web server.
- User accounts on the Oracle database are locked out after a number of invalid attempts to log in.
- VIS passwords are encrypted when making database connections.

Conclusion

VIS supports the SAVE program by providing automated status verification information to Federal, State, and local benefit-granting agencies. VIS also provides employment verification information to private Employers in various SAVE-sponsored Employment Verification Pilots.

For VIS, additional security measures and reporting capabilities have been introduced, new public access has been developed, and new interagency uses have been identified. No non-mitigated risks associated with personally identifiable information are identified because new users must undergo the same SAVE and VIS security procedures as previous users. Although use and disclosure of personally identifiable information is broader due to an expanded user base, SAVE and VIS security measures ensure each new member will access only the information to which they are entitled. This is accomplished through policies and the role-based access control scheme, which are supported by an audit process. Additionally, all users must complete training regarding policies and security requirements. Where data is shared outside of DHS, an MOU must be in place, which addresses the use of VIS, handling of account information, and security compliance requirements. These measures are in place to protect the data and identities of individuals in the system.

Responsible Officials

Gerry Ratliff, Chief, Verification Division, USCIS

Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security