Privacy Impact Assessment
for the

Humanitarian Adjudication for Victims Enterprise Nationwide (HAVEN)

March 11, 2011

Contact Point
Donald Hawkins, Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
(202) 272-1513

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

Abstract

The United States Citizenship and Immigration Services (USCIS) developed the Humanitarian Adjudication for Victims, Enterprise, Nationwide (HAVEN) to serve as a centralized case tracking database. The HAVEN supports the Victims of Trafficking and Violence Protection Action of 2000 mission area and the data and rules specific to this area. The HAVEN is a web-based application that supports the Vermont Service Center. HAVEN facilitates the processing of VTVPA petitions. HAVEN is a centralized repository of data for workflow management and production evaluation providing visibility into the processing of VTVPA cases. As a case management system, HAVEN streamlines workflow processing, notice generation and reporting for Adjudication Officers (AO) at the Vermont Service Center. HAVEN provides for the intake, receipting, and tracking of petitioner information through automated data processing. HAVEN allows the Adjudication Officers (AO) to efficiently adjudicate cases through a user-friendly interface. This PIA is being conducted because HAVEN uses Personally Identifiable Information (PII).

Overview

HAVEN provides a secure web-based application for case intake of immigration applications/petitions from around the world. This method of case management tracks the status of each case from intake to final Adjudication. To include intake, case assignment to an Adjudicator, leading to final Adjudication, correspondence created and correspondence received, viewing case data and reporting used for management planning.

Data included in each case record includes The HAVEN database will maintain information derived from the immigration forms for VTVPA benefits. These data elements include the self-petitioner's name, safe address (not necessarily the petitioner's residential address, but it could be the address of the attorney or representative), gender, marital status, country and date of birth, country of citizenship, passport number, passport issue date, passport issue place, I-94 number, date of last entry, place of last entry, current status and the HAVEN User ID. PII Data is not shared outside of USCIS. Case status is shared with Immigration and Customs Enforcement (ICE).

The HAVEN system processes include:

- Management of VTVPA casework.
- Case status tracking with audit trail capabilities.
- Correspondence and knowledge-management capability for storing and filling letter, memo, fax and correspondence templates.
- Regular and flexible multi-variable selection report generation.

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?

The system is used to collect applicant/beneficiary information used to process VTVPA petitions. This information is used soley by USCIS to determine the eligibility of the applicant to receive immigration benefits.

USCIS Employee information is collected in order to create system user accounts. This information is used to assign user's role and during system authentication and audit trail processes.

HAVEN contains the following personal data elements for the following purposes:

HAVEN User ID: USCIS Employee's First and Last Names, Middle Name, Claims User ID.

Applicant's Names: USCIS collects names (First, Last, and Middle) and aliases for applicants and family members, contact information of the attorney or representative and the preparer of the application in HAVEN.

Information Regarding Immigration Status: USCIS collects information relating to immigration status such as A-Number, I-94 Number, date of last entry, place of last entry and current status are entered into HAVEN as part of the application process.

Safe Addresses: USCIS collects the address of petitioner in HAVEN. Not necessarily the petitioner's residential address, but could be the address of the attorney or representative.

Telephone Numbers: USCIS collects telephone numbers of the applicant and preparer in order to have a secondary means of contacting either when needed to collect or provide information.

Birth Dates: USCIS collects birth dates (applicant, petitioner, spouse, children/stepchildren/adopted children) and enters them into in HAVEN.

Social Security Numbers: USCIS collects Social Security numbers (applicant and spouse) and enters them into HAVEN. This information is used to identify the self-petitioner's A-Number if one was not provided on the petition.

Citizenship/Nationality Information: USCIS collects information on the applicant's country of nationality, country of birth, province of residence in home country, passport number, passport issue date and languages spoken.

Marital Status: USCIS collects information regarding marital status (i.e., whether applicant is married, single, widowed, or divorced) and enters this information into HAVEN.

Gender: USCIS collects the genders of the applicant and dependents and enters them into HAVEN.

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

The HAVEN system data is manually entered based on the information submitted on USCIS application forms. USCIS employee data is manually entered by the employee, user account data is manually entered by the employee's supervisor and employee audit trail data is system generated.

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

HAVEN collects, stores and processes PII in order to provide a centralized and streamlined approach to case management. The HAVEN system provides management with real-time case statistics. The HAVEN system identifies deficiencies of cases and provides the status of those cases.

1.4 How is the information collected?

The data is collected from application forms submitted by applicants seeking immigration benefits. USCIS Employees manually enter the information from these forms into HAVEN.

1.5 How will the information be checked for accuracy?

Applicant information contained in HAVEN is checked for accuracy by an Adjudication Officer through the examination process. The HAVEN record for each case is subject to supervisory review prior to a final determination. Records are also subject to review by Headquarters for cases which require quality assurance review. The applicant's information (including biographical data, claim and immigration history) is verified and, if necessary, corrected on the form as well as in HAVEN based on any new information obtained during the adjudication. Corrections are also made if found during supervisory or headquarters review.

HAVEN is designed to require specific entries in the sequence outlined by the operating procedures to prevent inconsistencies in applicant data and in decision processing entries. HAVEN accomplishes this through program coding that allows or prevents record updates based on defined parameters. Similar edits exist for case closures, case transfers, file maintenance and many other case processing tasks.

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

The legal authority for HAVEN is derived from 8 United States Code (U.S.C.) Section 1101 et seq. More specifically, 8 U.S.C. Section 1103 charges the Secretary of the Department of Homeland Security (DHS) with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens.

USCIS collects the data from immigration forms filed by individuals seeking immigration benefits. As part of completing these forms the petitioner agrees to the provisions listed on the form.

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

Privacy Risk: HAVEN presents a risk of data inaccuracy.

Mitigation: The accuracy of this data is limited by the accuracy of the data entered on the immigration form and when information from the immigration form is manually entered into HAVEN. Adjudicators compare the data in HAVEN to the hard copy file. If discrepancies are found, HAVEN is updated with the correct information.

During a case review, if an Adjudicator discovers derogatory information, an intent to deny the benefit form is produced and sent to the applicant who has 30 days to respond. If a petition contains inaccurate data, the petitioner may rebut the intent to deny the benefit by responding to the request for additional evidence sent out by the Adjudicator assigned the case.

As a part of the case management tool, management tracks and reviews all user actions within HAVEN. This ensures that actions taken on the HAVEN system are reviewed for efficient case management and for possible misuse or inappropriate access to data.

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 HAVEN provides the following uses of the collected PII data:

- HAVEN utilizes PII obtained to process immigration applications for the VTVPA . The PII is used to identify and link multiple petitions to one person and family members of that person and determine the status of those cases. The benefit of this linkage is that all petitions by this applicant are processed in an orderly and efficient manner.
- PII is also used in identifying individual cases with deficiencies that are being held up as unworkable until those deficiencies are corrected. HAVEN identifies deficiencies and provides management reporting used for case management purposes of these cases.
- HAVEN also serves as a case status tool used to track the current stage a case is in and the time spent processing each stage of a case.

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

Microsoft SQL Server 2005 Enterprise Edition is utilized to manage, analyze and produce data such as reports for specific database size and performance.

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

The HAVEN system does not use commercially or publically available information.

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

Privacy Risk: The HAVEN data is subject to any of the following privacy risks:

- Breach of server/computer room by unauthorized personnel.
- Hacking.
- Intrusion into the network by unauthorized users.
- USCIS users leaving workstations unlocked and HAVEN client left open.
- Theft of backup tapes.

Mitigation: The following mitigations are in place to ensure that none of these risks are breached:

- User access is controlled by:
- USCIS Domain access is required prior to gaining access to HAVEN, which requires username/password, also if remote access is required the use of RSA Token and Virtual Private Network (VPN) to CISNET is used.
- HAVEN is a password protected system and therefore, their network credentials are required for CISNET access and also required in order to access HAVEN.
- Internal controls within HAVEN which ensure role-based access control and limit authorized users to specific areas of the data on a "need to know" basis only to protect privacy.
- Physical controls include a locked, caged data center with a halon system, biometric entry controls, security guards, and other security controls for controlled access.
- All HAVEN servers are configured according to the DHS baseline configuration guides, which include very strict controls for auditing and access control mechanisms. All DHS hardening standards were applied to both the Web Server OS and the Microsoft SQL Server 2005 Enterprise Edition package.
- Network Intrusion Detection System/Host Based Intrusion Detection Systems, Firewalls, anomaly detection, administrative safeguards and extensive training are also utilized for HAVEN. The HAVEN system resides behind a firewall and is constantly monitored by USCIS IT security staff.
- The HAVEN system is in the CISNET Domain and conforms to all standards of the DOMAIN.

- Backup tapes are only stored within the locked Verizon cage or within a fireproof locked vault at First Federal in Gaithersburg, Maryland.

Section 3.0 Retention

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

3.1 How long is information retained?

Automated A-File records will be maintained for 25 years after the case is closed, and then archived at the DOJ Data Processing Center or its designated successor for 75 years and then destroyed. Copies of system data may be stored in the individual's paper A-File (NCI-85-80-5/1). USCIS retains information generated by HAVEN reports for only as long as is necessary to support the agency's mission. Reports are never archived longer than the approved retention schedule period.

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

A retention schedule will be submitted to the NARA and as part of the Certification and Accreditation process.

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

Privacy Risk: Retaining data in HAVEN longer than necessary would violate the Fair Information Practice that requires the retention of the minimum amount of information necessary to perform relevant governmental functions.

Mitigation: Although there is always risk inherent to retaining data for any length of time, the HAVEN data retention periods are consistent with the concept of retaining data only for as long as necessary to support the agency's mission. The schedule proposed and awaiting approval by NARA complies with the requirements of the Federal Records Act and the stated purpose and mission of the systems. This system is a temporary solution that is designed to last five years in which time it is scheduled to be replaced. Therefore the records in Haven would be transferred to the new system.

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?

The information collected, processed and stored by HAVEN is only shared within the USCIS community.

4.2 How is the information transmitted or disclosed?

The HAVEN user interface is Web based and transmitted within the LAN. Only USCIS employees have access to the applicant data.

All users are provided extensive training handling privacy data. Any output from the HAVEN system comes with this warning:

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

Privacy Risk: The primary risk is unauthorized access to, or disclosure of, information contained within the systems.

Mitigation: Privacy Information in HAVEN is safeguarded in accordance with applicable laws, rules, and policies as discussed in more detail below.

Confidentiality Provisions of 8 CFR § 208.610:

Asylum-related data, in particular, is governed by strict regulatory confidentiality provisions outlined in 8 CFR § 208.6, Disclosure to Third Parties. This regulation generally prohibits the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations -- including information contained in HAVEN except under certain limited circumstances. This regulation safeguards information that, if disclosed publicly, could subject the claimant to retaliatory measures by government authorities in their home country or non-state actors in the event that the claimant is repatriated, or endanger the security of the claimant's family members who may still reside in the country of origin. Moreover, public disclosure might give rise to a plausible protection claim where one would not otherwise exist by bringing an otherwise ineligible claimant to the attention of the government authority in the applicant's home country or a non-state actor against which the claimant has made allegations of mistreatment.

According to established interpretative guidance, confidentiality is breached when information contained in or pertaining to an asylum application (including information contained in HAVEN) is disclosed to a third party in violation of the regulations, and the unauthorized disclosure is of a nature that allows the third party to link the identity of the applicant to: (1) the fact that the applicant has applied for asylum; (2)

specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or (3) facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum. The same principles govern the disclosure of information related to credible fear and reasonable fear determinations, as well as to applications for withholding or deferral of removal under Article 3 of the Convention against Torture, which are encompassed within the asylum application.

In the absence of the asylum applicant's written consent or the DHS Secretary's specific authorization, disclosure to third parties may be made only to United States government officials or contractors and United States federal or state courts on a need to know basis related to certain administrative, law enforcement, and civil actions. In some instances, interagency arrangements have been established - such as the arrangement between the former INS and the FBI -- to facilitate the proper disclosure of asylum-related information to United States agencies pursuant to the regulations. The release of information relating to an asylum application, credible fear determination, or reasonable fear determination (including information contained in HAVEN) to an official of another government or to any entity for purposes not specifically authorized by the regulations without the written consent of the claimant requires the express permission of the DHS Secretary.

Privacy Safeguards of DHS and USCIS:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need to know. This adheres to requirements of the DHS Information Technology Security Programs Handbook to employ password protection identification features to protect sensitive information. All internal components are mandated by DHS to comply with DHS' Sensitive System Security guidelines.

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

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?

N/A. HAVEN data is not shared outside of USCIS.

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.

N/A. HAVEN data is not shared outside of USCIS.

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

N/A. HAVEN data is not shared outside of USCIS.

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

N/A. HAVEN data is not shared outside of USCIS.

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?

A System of Records Notice (SORN) for HAVEN will be published in the Federal Register if a determination is made one is needed.

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e) (3)[1] of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested and to use the data to populate immigration forms and in support of an application. The forms also contain a provision by which an petitioner authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

[1] The USCIS Privacy Policy can be found at: http://www.uscis.gov and on the instructions that accompany each form.

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

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e) (3)[2] of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested and to use the data to populate immigration forms and in support of an application. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

All individuals applying for immigration benefits and providing information have the right to consent or deny particular uses of the information by either not signing a release authorization or by dropping their immigration request.

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

USCIS benefit applications require that applicants provide certain biographic and biometric information that may include submission of fingerprints, photographs, and signatures in addition to other information requested in an application. This information is critical in making an informed adjudication decision to grant or deny a USCIS benefit. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes. Specifically, all USCIS immigration forms include a Privacy Act Statement and require the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." USCIS forms also contain a statement notifying applicants that their information may be shared with other federal agencies as well. This information is also conveyed in the Privacy Act Statement on the application itself. Applicants are provided an opportunity to review how their information will be used and shared. Individuals grant consent to the collection and use of the information when they sign the application.

All individuals applying for immigration benefits and providing information have the right to consent or deny particular uses of the information by either not signing a release authorization or by dropping their immigration request.

[2] The USCIS Privacy Policy can be found at: http://www.uscis.gov and on the instructions that accompany each form.

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.

The individual(s) immigration request clearly identifies the collection and use of PII data and contains a disclaimer on the individual immigration forms signed (either physically or electronically) by the requestor.

Applicants for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for immigration benefits. Each immigration form contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants are also advised that the information provided will be shared with other Federal, state, local and foreign law enforcement and regulatory agencies during the course of the investigation. In the USCIS website Privacy Notice,10 individuals are also notified that electronically submitted 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 (FOIA). OMB approved all Privacy Act Statements used when collecting data.

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?

An individual who is the subject of a record in HAVEN may access those records that are not exempt from disclosure. A determination whether a record may be accessed (by the individual or others) will be made at the time a request is received based on FOIA exemptions or Privacy Act exemptions claimed in the SORN.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064-8010. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "contacts."

When seeking records about yourself from this system of records or any other USCIS system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, USCIS will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

The accuracy of this data is limited by the accuracy of the data entered on the Immigration form and when information from the Immigration form is manually entered into HAVEN. Adjudicators compare the data in HAVEN to the hard copy file. If discrepancies are found, HAVEN is updated with the correct information.

During a case review, if an adjudicator discovers derogatory information, a request for evidence form is produced and sent to the applicant who has 30 days to respond. If an application contains inaccurate data, an applicant may rebut the intent to deny the benefit or respond to the request for additional evidence sent out by the adjudicator assigned the case.

Computer Security Awareness training is provided on an annual basis and HAVEN users are frequently trained through USCIS Academy and provided a computer based tutorial from which to refresh their awareness.

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

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

This PIA also provides similar notice. Privacy Act Statements, including notice of an individual's right to correct information, are also contained in immigration forms published by USCIS.

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

USCIS provides formal redress for individuals wishing to correct information HAVEN.

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

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

Privacy Risk: The main risk with respect to redress is that the right may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the system. Individuals are given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources. Individuals may avail themselves of the redress and appeal process as stated in the DHS Privacy Act regulations (found at 6 Code of Federal Regulations, Section 5.21).

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 HAVEN system utilizes Active Directory to determine which users may access the system. Current HAVEN users are already set up in Active Directory and the security policies relating to their user profile will determine their ability to access HAVEN. Within the HAVEN system; users are assigned a specific role which determines their access in terms of specific HAVEN functionality.

8.2 Will Department contractors have access to the system?

Contractors are also assigned by roles with limited access to HAVEN data; such as authorization for data entry.

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

Computer Security Awareness training is provided on an annual basis and HAVEN users are frequently trained through USCIS Academy and provided a computer based tutorial from which to refresh their awareness.

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

The HAVEN system is currently undergoing the C&A process and will not be connected to the network until an Authority to Operate (ATO) has been granted. Completion of the HAVEN C&A is expected by October 2011.

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

The HAVEN system has internal audits separate from the domain security audits; therefore, a double layer of audit trails exist.

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

Privacy Risk: Given the scope of the personal information in HAVEN, the security of the information on the system is of critical importance. Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing) that require mitigation.

Mitigation: To mitigate these risks, a number of business and systems rules have been implemented. Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, misuse and inappropriate dissemination of data. Access to the database is given only to users that need it to perform their official duties. All authorized users must authenticate using a user ID and password. Role-based user accounts are used to minimize the number of persons who have access to the system. Audit trails are kept in order to track and identify any unauthorized changes to information in the system. The HAVEN has a comprehensive audit trail tracking and maintenance function that stores information for every action taken.

The following user roles are utilized for the HAVEN:

User Role Number	User Type or Job Title	Description of Duties / Responsibilities
1	Administrator	• All rights • Create User Profiles according to user roles • Maintain User Profiles • Deactivate / Reactivate User Profiles • Maintain Tables • Set cap
2	VSC Supervisory ISO (SISO)	• Reviews and edits ISO2 adjudication entries. • Must have both read, write and void capabilities
3	VSC ISO 1	• Processes customer inquiries • Must have the ability to update • Must have the ability to make corrections (i.e. Validity dates, classification, Name, DOB, etc.)
4	VSC ISO 2	• All adjudicative functions • Must be able to read, update, void, approve, deny and edit records
5	VSC ISO 3	• All adjudicative functions • Must be able to read, update, void, approve, deny and edit records • Similar to the access of an SISO • Maintain tables • Approve cases over 'cap minus reserve'
6	VSC Contract Data Entry Supervisory	• Reviews the Data Entry Clerks work • Must have void capability
7	VSC Contract Data Entry Clerks	• Data enters forms • Access will be limited to those form types the user is currently trained in processing
8	VSC Data Reporting Group	• View only • Reporting capabilities
9	Basic user (no rights)	• View only

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 HAVEN system is a case processing system that utilizes workflow, reports current case status and reports staffing levels.

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

HAVEN is currently in the Development stage and is scheduled for release October 11, 2011. HAVEN utilizes the Systems Engineering Life Cycle (SELC) lifecycle methodology.

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

The technologies used conform to USCIS Enterprise Architecture and Engineering group standards, web system standards and approved development, test and staging environments in the Standard Lightweight Operational Programming Environment (SLOPE) used to develop the HAVEN system.

Approval Signature Page

_____

Chief Privacy Officer
Department of Homeland Security