Privacy Impact Assessment
for the

Validation Instrument for Business Enterprises (VIBE)

DHS/USCIS/PIA-044

April 15, 2014

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8000

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), United States Citizenship and Immigration Services (USCIS) Service Center Operations Directorate (SCOPS) developed the Validation Instrument for Business Enterprises (VIBE) system. USCIS SCOPS uses VIBE to (1) validate the business operations and financial viability of organizations seeking to employ foreign workers; and (2) identify benefit fraud based on the Fraud Detection and National Security Directorate (FDNS) findings and other government agencies' referrals. USCIS is conducting this Privacy Impact Assessment (PIA) because VIBE collects, uses, and disseminates personally identifiable information (PII).

Overview

The United States Citizenship and Immigration Services (USCIS) is the component of the Department of Homeland Security (DHS) that oversees lawful immigration to the United States. Within USCIS, the Service Center Operations Directorate (SCOPS) oversees the timely administration and adjudication of immigration benefits at its Service Centers and the Fraud Detection and National Security Directorate (FDNS) is responsible for detecting, deterring, and combating immigration benefit fraud. Both SCOPS and FDNS collaboratively strive to strengthen national security and the integrity of the legal immigration system, while simultaneously supporting the administration of immigration benefits in a timely and effective manner.

USCIS processes thousands of applications, requests, and petitions submitted by applicants, requestor, petitioners, and organizations (petitioning entity) every year. Often, petitioning entities are required to submit completed filings along with additional background documentation to establish benefit eligibility. As part of the adjudication process, Immigration Services Officers (ISOs) substantiate the submitted information and conduct security screening checks.[1] ISOs refer cases suspected of possible immigration benefit fraud to FDNS Immigration Officers (FDNS IO) at Center Fraud Detection Operations (CFDO) to initiate an administrative inquiry.[2] This process helps to ensure the integrity of the immigration process.

USCIS SCOPS operates the Validation Instrument for Business Enterprises (VIBE) as an additional tool for ISOs to use in adjudicating employment-based benefits and other benefits that are associated with a higher fraud risk, such as Deferred Action for Childhood Arrivals.[3] VIBE

[1] *See* DHS/USCIS/PIA-033 - Immigration Benefits Background Check Systems (IBBCS), *available at* www.dhs.gov/privacy.
[2] FDNS IOs are located at all USCIS service centers, field offices, asylum offices, and some overseas offices. FDNS IOs are responsible for conducting administrative inquiries into suspected benefit fraud and aiding in the resolution of national security or criminal concerns. *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Directorate (FDNS), *available at* www.dhs.gov/privacy.
[3] *See* Appendix A for a list of petitions and applications used to identify ineligible petitioning entities, immigration

streamlines the adjudication of certain employment-based immigration petitions by prescreening the data received from the petitioning entity, or the petitioning entity's attorney or accredited representative. VIBE-processed benefit requests may receive a commercial source check or a known fraud list check before moving to ISO review. The ISO may adjudicate the petition or refer it to CFDO for further investigation before adjudicating the case.

Commercial Source Check

USCIS uses commercial information to verify a petitioning entity's qualifications for the benefit requested, to assess a petitioning entity's financial viability for cases that require the petitioning entity to establish ability to pay, and to provide a basis for a score that assists ISOs in identifying possible fraud concerns or contradictory information submitted by the petitioning entity. VIBE submits the petitioning entity's name and address to Independent Information Provider (IIP), currently Dun and Bradstreet (D&B) to retrieve commercially-available data on the petitioning entity. Since D&B only provides information on businesses and the executives of those businesses, individual petitioner information will likely not result in a match against D&B. If a search against D&B does not result in a match, VIBE moves the benefit request to the next verification, the known fraud lists (discussed below).

If VIBE finds a match in the D&B database, VIBE retrieves the following D&B information:

- D-U-N-S® Number (company unique ID received from the IIP)
- Global Ultimate D-U-N-S® Number
- Global Ultimate company name
- Global subsidiary (e.g., company hierarchy, parent organizations, subsidiary organizations, and affiliate organizations)
- Foreign relationships
- Legal Status (e.g., LLC, LLP, Partnership, Sole-Proprietorship, non-profit)
- Trade styles, which are additional names used by a business for advertising or buying purposes
- Location type (e.g., Branch Office, Subsidiary, Headquarters)
- Type of business
- Total number of employees employed at a particular location
- Total number of employees by the petitioning organization worldwide

---

practitioners, and addresses. *See* DHS/USCIS/PIA-045 – Deferred Action for Childhood Arrivals (DACA), *available at* www.dhs.gov/privacy.

- Year established
- Import/Export business type
- Number of related entities
- Number of corroborating sources, which indicates the number of authenticating source types that provide corroboration of a business's identity and existence
- Tax exempt indicator
- Year the current owners took control of the organization
- Annual gross sales volume (modeled, actual, or estimated)
- Payment history of the petitioning organization to include total payments and timeliness of payments
- Company executive names and titles
- Business activity indicator, which is an indicator that measures the likelihood that the company is no longer in business. This indicator could be based on Uniform Commercial Code (UCC) filings, lack of activity, etc.
- A financial risk indicator, which measures the likelihood that the company will cease operations as a going concern within the next 12 months.

VIBE consolidates petitioning information and the information retrieved from D&B to create a VIBE Status Report (VSR). In addition to D&B data, the VSR includes basic petition information (e.g., receipt number, visa type, receipt date, record timestamp, adjudicative status, petitioning company or organization, company address) and the VIBE Scoring Result.

The VIBE Scoring Result is a risk-based score that notifies the ISO of any potentially problematic areas in the petition. The VIBE Scoring Result may also be affected if petition information or the petitioning entity is on a known fraud list. VIBE creates the VIBE Scoring Result by using a series of specially designed algorithms and comparing commonalities and differences between USCIS and D&B data.[4] USCIS does not make an automatic decision based solely on the VIBE Scoring Result. USCIS granted CBP access to VIBE to assist in visa petition processing and to promote program integrity. CBP officers may enter an approved petition receipt number in VIBE to generate a VSR.

[4] Information from D&B is scored using a customized scoring algorithm, and is integrated with other information from the petition, information on the FDNS benefit fraud analysis, and information on USCIS experiences with past petitions (including problems previously encountered). The result of the algorithm is displayed to the adjudicator as part of a consolidated, comprehensive report.

Known Fraud Lists Check

Simultaneous with VIBE retrieving any commercially available data on the petitioning entity, VIBE checks whether the petitioning entity matches an entry on a known fraud list. A known fraud list is a compilation of confirmed fraud, criminal activity, public safety, or national security concerns that are associated with an entity, immigration practitioner, or address. An entity, immigration practitioner, or address may be added to the list when one of the following criteria is met: currently the subject of an administrative investigation, suspended from filing with USCIS, debarred by the Department of Labor (DOL) for violating the Immigration and Nationality Act (INA), the subject of Department of Justice (DOJ) Executive Office of Immigration Review (EOIR) disciplinary action, or the subject of an ongoing criminal investigation. If information on a benefit request matches an entry on a known fraud list, VIBE alerts the ISO by overriding the VIBE Scoring Result to show that the petition should be referred to CFDO for further investigation. The FDNS PIA covers CFDO's investigation regarding the known fraud lists.[5]

SCOPS receives known fraud list referrals from the following sources:

1. **USCIS CFDO Referrals**: A CFDO IO may make a referral when he or she identifies a petitioning entity, immigration practitioner, or address that is currently a subject of an administrative investigation, is suspended from filing with USCIS, is the subject of an ongoing criminal investigation, or has a conviction for immigration fraud.
2. **DOL Debarment**: When DOL determines that an organization has violated the INA, the organization is subject to a mandatory debarment. USCIS will not approve petitions filed by the debarred organization during the debarment period. Therefore, when USCIS receives a debarment notice from DOL, SCOPS places the debarred organization on a known fraud list until the debarment period expires.[6]
3. **DOJ List of Currently Disciplined Practitioners**: The DOJ EOIR Attorney Discipline Program maintains a publically available list of currently disciplined immigration practitioners. This list includes the immigration practitioner's name, city and state, date immediate suspension imposed, final discipline imposed, effective date of discipline, and whether the practitioner was reinstated. USCIS receives the list of currently disciplined practitioners directly from DOJ. SCOPS places the disciplined practitioners on a known fraud list until practitioner is reinstated.[7]

---

[5] *See* DHS/USCIS/PIA-013(a) FDNS, *available at* www.dhs.gov/privacy.
[6] DOL posts a list of debarred organizations at http://www.dol.gov/whd/immigration/H1BDebarment.htm and http://www.foreignlaborcert.doleta.gov/pdf/Debarment_List_Revisions.pdf.
[7] DOJ posts a list of currently disciplined practitioners at http://www.justice.gov/eoir/discipline.htm. *See* JUSTICE/EOIR-003 Practitioner Complaint Disciplinary Files SORN, *available at* http://www.justice.gov/opcl/privacyact.html#EOIR.

4. **USCIS FDNS Administrative Site Visit and Verification Program (ASVVP) Compliance Review:** All USCIS religious worker petitions[8] are required to comply with the ASVVP Compliance Review. A religious organization will be placed on a known fraud list, if the result of ASVVP returns as "Compliance Review Failed"[9] and "fraud found."[10]

5. **Law Enforcement Agency (LEA) or other government agency referrals**: Agencies, such as U.S. Immigration and Custom Enforcement (ICE) and Department of State (DOS) Diplomatic Security and Consular Affair Fraud Prevention Program, refer entities, individuals, and addresses to a known fraud list based on their fraud validation process.

The known fraud list referral form generally collects: name of the petitioning entity or immigration practitioner, address, the receipt number for the petition filed by the petitioning entity (if any), the corresponding USCIS Fraud Detection and National Security – Data System[11] (FDNS-DS) record number, [12] the unique identifier assigned by D&B for an entity (D-U-N-S® Number), the reason for the referral, and the source of the referral. The information on the known fraud list is based on the findings and research conducted by FDNS, DOL, DOJ EOIR, law enforcement agencies (LEA), or other government agencies.

SCOPS Headquarters reviews each known fraud list referral to ensure the referred case meets the criteria for being placed on one of the lists. Once vetted and confirmed for fraud, the referred petitioning entity, immigration practitioner, or address is manually entered into one of three separate searchable known fraud lists:

1. **Known Fraud Entities**: All entities identified as committing fraud through an administrative inquiry or DOL debarment are added to this list. Known fraud entities may include businesses, organizations, and educational institutions identified as "diploma mills."[13] This list generally maintains the name of the entity, associated FDNS-DS

[8] *See* 8 CFR § 204.5(m).
[9] "Compliance Review Failed" is used to describe the results of a compliance review where FDNS has determined that there was a material misrepresentation or other non-compliance that was germane to the adjudication of the benefit. In order for a determination of failed to be made, the FDNS IO must have sufficient evidence of fraud or non-compliance to support a denial, Notice of Intent to Deny (NOID), revocation, Notice Of Intent to Revoke (NOIR), or Notice To Appear (NTA).
[10] The ASVVP conducts site inspections to verify information, better identify fraud cases for follow-up, and when appropriate, refer cases to ICE for investigation. All religious organizations are subject to site inspections/compliance reviews prior to adjudication of Form I-360 or Form I-129.
[11] *See* DHS/USCIS/PIA-013 Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy. *See also* DHS/USCIS-006 – FDNS Records, 77 FR 47411(Aug. 8, 2012).
[12] An FDNS Record Number is a number that is automatically generated by FDNS-DS upon the creation of a new record.
[13] According to the United States Department of Education, Higher Education Opportunity Act, the term `diploma mill' means an entity that (A)(i) offers, for a fee, degrees, diplomas, or certificates, that may be used to represent to the general public that the individual possessing such a degree, diploma, or certificate has completed a program of postsecondary education or training; and (ii) requires such individual to complete little or no education or

record, and a brief reason for its inclusion on the list.

2. **Known Fraud Immigration Practitioners**:[14] An attorney or an accredited representative can act on behalf of an applicant, petitioner, or requestor by completing a DHS Form G-28, *Notice of Entry of Appearance as Attorney or Accredited Representative*. An attorney or an accredited representative of a recognized organization may represent an applicant, or petitioning entity seeking immigration benefits without the appropriate credentials to perform this service. Immigration practitioners on this list have been the subject of federal, state, or local court action to stop their unauthorized practice of law or theft of fees for legal services. This list generally maintains the name of the immigration practitioner, the state abbreviation of the immigration practitioner's address, associated FDNS-DS record, and a brief reason for the practitioner's entry on the list.

   Information in this list is retrieved by "soundex," a phonetic algorithm for indexing names by the way they sound instead of the way they are spelled. A soundex hash is a code that weighs the sounds of letters so that similar sounding names, recorded under various spellings, result in the match. A soundex hash of the first and last name will be compared to a soundex hash of known fraud immigration practitioners. VIBE automatically runs a soundex query only when a petition, request or application is filed with Form G-28. When the VIBE system perform the soundex query, the system will fetch the immigration practitioner name and state abbreviation based on the G-28 information and bounce against the Known Fraud Immigration Practitioners list to identify possible matches. Only the matched Known Fraud Practitioners, the corresponding FDNS-DS record number, and a brief reason for why the immigration practitioner is on the list are displayed in VIBE.

3. **Known Fraud Addresses**: USCIS also identifies addresses associated with multiple filings by one or more organization, attorney, preparer, law office, applicant, or petitioner that FDNS suspects or finds to have engaged in fraud, criminal activities, or when national security concerns are present.

   This list includes physical addresses and mailing addresses. FDNS provides the initial list of Known Fraud Addresses based on the records in FDNS-DS for individuals who USCIS suspects or finds to have engaged in the fraud with the associated address. Only the matched Known Fraud Addresses, the corresponding FDNS-DS record number, and a brief reason for why the address is on the list are displayed in VIBE.

   USCIS maintains the three lists in Enterprise Citizenship and Immigrations Services

---

coursework to obtain such degree, diploma, or certificate; and (B) lacks accreditation by an accrediting agency or association that is recognized as an accrediting agency or association of institutions of higher education (as such term is defined in section 102) by-- (i) the Secretary pursuant to subpart 2 of part H of title IV; or (ii) a Federal agency, State government, or other organization or association that recognizes accrediting agencies or associations.

[14] *See* DHS/USCIS-006 – FDNS, 77 FR 47411(Aug. 8, 2012).

Centralized Operational Repository (eCISCOR) for VIBE retrieval and use.[15] All VIBE data is stored in the VIBE tablespace within the eCISCOR. The Form G-28 is data entered in CLAIMS 3 and stored in eCISCOR. When VIBE performs the soundex query on G-28 data, the immigration practitioner's name and state abbreviations based on G-28 data is copied and stored temporarily in the VIBE tablespace. Once the soundex query is executed for each newly filed application, request or petition, the temporary G-28 query data will be deleted permanently from the VIBE tablespace. SCOPS also maintains and stores the master known fraud list on the USCIS SharePoint Electronic Collaboration Network (ECN) site for the purposes of record management and data integrity.[16] The ECN allows SCOPS to note when a document is loaded onto the site, and SCOPS site administrators regularly review the creation date of content and remove it when the retention period expires. The SCOPS ECN site is protected using security safeguards established by DHS and is restricted to authorized employees who have a need-to-know. Other USCIS or other agency personnel do not have access to the copy maintained on the ECN site and this copy is not connected in any way electronically or otherwise to the VIBE system.

A known fraud entity, known fraud immigration practitioner, or known fraud address placed by USCIS on a known fraud list includes a validity period for remaining on the list. The validity period for DOL debarred organizations or DOJ EOIR disciplined attorneys list is based on the duration of the debarment or the status of reinstatement.

Other than the DOL debarred organizations or DOJ EOIR disciplined attorneys list, a known fraud entity generally has an initial validity period of five years. Due to the severity of the fraud activities committed by the known fraud entities, the validity period for remaining on a known fraud list can also be extended upon CFDO's request. However, if at any time CFDO finds that an entity should no longer be considered a known fraud entity, CFDO can also request to remove the entity from a known fraud list. SCOPS has established a known fraud list procedure for checking the validity period. SCOPS and CFDO review the fraud status of each known fraud entity 30 days before the validity period expires to determine if the validity period needs to be extended.

Once VIBE checks the petition against commercially-available data and the known fraud lists, the ISO is ready to review the VIBE Status Report and the supplemental information provided with the petition. If information on a petition matches an entry on a known fraud list, then the petition moves to the third verification—CFDO investigation. If the petition information does not match an entry on a known fraud list, the VIBE inquiry is complete and the

[15] *See* DHS/USCIS/PIA-023 - Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy. *See also* DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS-USCIS-007 - Benefits Information System, 73 FR 56596 (September 29, 2008).
[16] *See* DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites PIA, *available at* www.dhs.gov/privacy.

ISO may continue moving the case towards final adjudication.

VSR Review

Once the ISO receives the VSR, he or she compares the petition and supporting evidence against the VSR to verify the financial viability and operational status of the petitioning entity. If the ISO discovers contradictory information that is material to the petition and not explained by the evidence submitted with the petition, USCIS may issue a Request for Evidence (RFE)[17] or Notice of Intent to Deny (NOID).[18] The RFE or NOID notifies the petitioning entity that USCIS found contradictory or derogatory information in VIBE. The RFE or NOID references the information VIBE received from D&B and requests for supporting documents to resolve USCIS's questions.[19] USCIS grants the petitioning entity an opportunity to overcome this determination and demonstrate that he or she is eligible. However, failure to respond to an RFE or NOID often results in the denial of a case. If derogatory information is detected, the ISO may refer the petition through VIBE to CFDO for further investigation.[20]

If the VSR indicates to the ISO that a petition was filed by a known fraud entity, from a known fraud address, or prepared by a known fraud immigration practitioner, the ISO refers the petition to CFDO for an administrative inquiry. An ISO also refers petitions to CFDO when he or she identifies derogatory information questioning the veracity of the petitioning entity or other individuals or organizations associated with the benefit being sought during the petition review process. All cases meeting the criteria for fraud must be referred to CFDO for review, even if there is sufficient evidence to deny the petition.[21] Examples of possible fraud indicators include unknown or unusual mailing address, multiple filings by petitioner inconsistent with company size, and discrepancies between claimed gross earnings and tax returns. Information collected during the administrative inquiry is entered into FDNS-DS,[22] reported back to SCOPS, and may be added to a known fraud list.

---

[17] An RFE is a formal statement issued on a pending case when the USCIS determines that additional clarification, information, or evidence is needed to approve the case.

[18] A NOID is a formal statement from USCIS that it has determined that the applicant is ineligible for the immigrant benefit requested. However, the USCIS will grant the applicant an opportunity to overcome this determination and demonstrate that he or she is eligible.

[19] USCIS also provides instructions on how to contact D&B that allow these USCIS petitioners to create, update, and view basic elements of their company's or organization's D&B report without being subjected to direct marketing from D&B. *See* www.uscis.gov/VIBE.

[20] *See* DHS/USCIS/PIA-013(a) FDNS, *available at* www.dhs.gov/privacy.

[21] Fraud is defined as willful misrepresentation or falsification of a material fact. Fraud entails any manifestation that amounts to an assertion not in accordance with the facts, an untrue statement or concealment of a material fact, and/or an incorrect or false representation material to the eligibility or adjudication of the petition. This definition is consistent with Immigration and Nationality Act § 212(a)(6)(C)(i), codified at 8 U.S.C. § 1182(a)(6)(C)(i), which states, "any alien who, by fraud or willfully misrepresenting a material fact, seeks to procure (or has sought to procure or has procured) a visa, other documentation, or admission into the United States or other benefit provided under this Act is inadmissible."

[22] *See* DHS/USCIS/PIA-013 FDNS-DS, *available at* www.dhs.gov/privacy.

USCIS may not deny a petition solely based upon information from VIBE, and will give the petitioning entity an opportunity to respond to USCIS's concerns. The ISO will make his or her final decision based on the totality of the circumstances. The petitioning entity may choose to contact D&B to update the petitioning entity's record to prevent any subsequently filed petitions from receiving a similar RFE or NOID for the VIBE-related issue in question. However, the petitioning entity must respond to USCIS with the information requested in the RFE or NOID regardless of whether the petitioning entity chooses to update its record with D&B. USCIS provides the petitioning entity with the opportunity to explain and resolve any inconsistencies prior to issuing an adjudicative decision. Updating the petitioning entity's record with D&B is not a substitute for responding to USCIS's RFE or NOID. Failure to respond to the RFE or NOID directly to USCIS may result in denial of the petition.

External Sharing

After USCIS approves the petition, the beneficiary applies for a visa with the Department of State (DOS). USCIS forwards the approved petitions to DOS for consular processing. This involves activities related to the visa interview and issuance process. A beneficiary of an approved petition may apply with DOS at a consulate abroad for a non-immigrant or immigrant visa to come to the United States to work or be admitted as a permanent resident. A visa allows a foreign citizen coming from abroad to travel to the United States. During this process, DOS reviews the most current information provided to determine whether the petitioning entity and beneficiary continue to be eligible for the classification for which approved by USCIS.

USCIS grants DOS access to VIBE through a secured Enterprise Service Bus (ESB) interface.[23] DOS-designated employees may access VIBE as a non-DHS user with a read-only user rights. VIBE information sharing between USCIS and DOS provides a comprehensive picture of the visa applicant's status to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 103 of the Immigration and Nationality Act provides the legal authority for this system.[24]

[23] *See* the DHS/USCIS/PIA-008 - Enterprise Service Bus (ESB), *available at* www.dhs.gov/privacy.
[24] 8 U.S.C. § 1103.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs cover the collection, maintenance, and use of VIBE:

- DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records[25] covers the petition, supplemental evidence, and decision notices;
- DHS/USCIS-006 Fraud Detection and National Security Records[26] covers the cases referred to CFDO for administrative inquiry and identified as benefit fraud; and
- DHS/USCIS-007 - Benefits Information System[27] covers the review of applications and petitions.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

VIBE is a service subsystem that falls under USCIS Enterprise Service Bus 2 (ESB 2) accreditation boundary. USCIS completed the USCIS ESB 2 system security plan on September 08, 2011. USCIS ESB 2, which includes VIBE, was approved for operation until August 29, 2015.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. USCIS is working with NARA to create a records retention schedule for VIBE. USCIS is proposing a retention period of 15 years for VIBE records, which is similar to the retention for the associated records found in FDNS-DS [N1-566-08-18] and Computer Linked Adjudication Information Management System 3 (CLAIMS 3)[28] [N1-563-04-03]. Once USCIS removes an entity, immigration practitioner, or address from a known fraud list, the information will be retained as historical data for 15 years from the date that the known fraud information is added into VIBE. Once the known fraud list entry expires, the associated known fraud list rule will not be used to generate new VSRs.

[25] DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).
[26] DHS/USCIS-006 FDNS Records, 77 FR 47411 (Aug. 8, 2012).
[27] DHS-USCIS-007 - Benefits Information System, 73 FR 56596 (Sept. 29, 2008).
[28] *See* DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3), *available at* www.dhs.gov/privacy. *See also* DHS-USCIS-007 - Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

There are no forms associated with this collection. However, SCOPS may use data from USCIS petitions that are subject to PRA and have assigned OMB Control numbers.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

VSR

The VSR is a detailed report that adjudicators use to validate the business operations of organizations seeking to employ foreign workers. Information in VIBE may include:

Information that applies to employment-based petitions (CLAIMS 3)

- Receipt number and date
- Petitioning entity's name
- Physical address or mailing address
- Adjudicative status
- Visa type
- Record Time-stamp
- Any associated receipt numbers up to 3 years of previous filings
- Immigration practitioner's name

Information that applies to employment-based petitions (D&B)

- D-U-N-S® Number (company unique ID received from the IIP)
- Global Ultimate D-U-N-S® Number
- Global Ultimate company name
- Global subsidiary (e.g., company hierarchy, parent organizations, subsidiary organizations, and affiliate organizations)
- Foreign relationships
- Legal Status (e.g., LLC, LLP, Partnership, Sole-Proprietorship, non-profit)

- Trade styles, which are additional names used by a business for advertising or buying purposes
- Location type (e.g., Branch Office, Subsidiary, Headquarters)
- Type of business
- Total number of employees at a particular location
- Total number of employees by the petitioning organization worldwide
- Year established
- Import/Export business type
- Number of related entities
- Number of corroborating sources, which indicates the number of authenticating source types that provide corroboration of a business's identity and existence
- Tax exempt indicator
- Year the current owners took control of the organization
- Annual gross sales volume (modeled, actual or estimated)
- Payment history of the petitioning organization to include total payments and timeliness of payments
- Company executive names and titles
- Business activity indicator, which is an indicator that measures the likelihood that the company is no longer in business. This could be based on UCC filings, lack of activity, etc.
- A financial risk indicator, which measures the likelihood that the company will cease operations as a going concern within the next 12 months

Information that applies to employment-based petitions (generated by VIBE)

- Match confidence score, which indicates how closely the petitioning entity matches the entity found in D&B's records.
- VIBE Scoring Result, which compares the petitioning entity data against an algorithm.
- "VIBE Pre-defined Company Score" section allows an ISO or FDNS IO to provide additional information about a petitioning entity that is pertinent to its validity or eligibility, or a brief description of the reason why a petitioner or applicant's VIBE overall score has been overridden. The information may contain the entity's financial viability information (e.g., company's ownership, company's foreign subsidiaries);

information about the individuals related to the entity (e.g., the owner, representative, attorney or preparer of the entity); or adjudicative notes based on FDNS findings and research in certain areas of the petition. This section may list corresponding FDNS-DS record numbers for possible fraud review. USCIS will not make an automatic decision based solely on this score.

Information that applies to individual-based petitions (CLAIMS 3)

- Receipt number and date
- Service Center
- Applicant address or mailing address if matching to the Known Fraud Address list
- Adjudicative status
- Form type
- Immigration Practitioner's name based on the Form G-28, *Notice of Entry of Appearance as Attorney or Accredited Representative*, if matching to the Known Fraud Immigration Practitioner list

The VSR is stored in the VIBE tablespace within eCISCOR.[29]

VIBE Known Fraud List

The VIBE program also incorporates a fraud detection process known as the VIBE known fraud lists that enable ISOs to identify if an entity, immigration practitioner, or address is (1) currently a subject of an administrative investigation, (2) suspended from filing with USCIS, (3) barred by the DOL, (4) the subject of disciplinary action by DOJ EOIR, or (5) the subject of an ongoing criminal investigation. The Known Fraud Entity list maintains the name of the entity; associated FDNS-DS record, if applicable; and the brief reason for the entity's inclusion on the list. The Known Fraud Immigration Practitioner list maintains the name of the immigration practitioner; the state abbreviation of the immigration practitioner's address, associated FDNS-DS record, if applicable; and the brief reason for the practitioner's inclusion on the list. The Known Fraud Address list maintains the address; associated FDNS-DS record, if applicable; and, the brief reason for its inclusion on the list.

VIBE retrieves certain newly filed applications, requests and petitions from CLAIMS 3 to vet against the Known Fraud Entities, Known Fraud Immigration Practitioners, and Known Fraud Addresses lists. Information retrieved by VIBE from CLAIMS 3 may include: (1) receipt number and date; (2) petitioning entity's name; (3) physical address or mailing address; (4)

[29] *See* DHS/USCIS/PIA-023 - Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy. *See also* DHS/USCIS-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS-USCIS-007 - Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

adjudicative status; (5) form type; (6) record time-stamp; (7) any associated receipt numbers up to 3 years of previous filings; and (8) immigration practitioner's name. The VIBE known fraud lists creates a report of every positive match against the three lists. The VIBE known fraud lists function displays the following information in the report:

- Receipt Number
- Petitioning entity/Immigration Practitioner Name
- Mailing or physical address
- Associated FDNS-DS number

2.2 What are the sources of the information and how is the information collected for the project?

The VIBE VSR collects and maintains information from a variety of sources to assess the financial viability and current level of business operations for the petitioning entity, and to use the result of that analysis as an input into the adjudication process of the employment-based petitions. VIBE electronically receives company information from D&B and the petition information from CLAIMS 3.

The VIBE known fraud lists maintain information on individuals, entities, and addresses associated with suspected or confirmed fraud, criminal activity, public safety, or national security concerns. The sources for the known fraud lists include: USCIS CFDO referrals, results of ASVVP Compliance Review, DOL, DOJ EOIR, LEAs, or other government agency referrals. Specifically, VIBE electronically receives certain newly filed application and petition information from CLAIMS 3 and vets it against the lists to identify possible matches.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

VIBE collects, maintains, and uses information from the following commercial and publicly available data providers:

- **The current IIP, D&B,** maintains a global database of companies and professional contacts. D&B shares this information with VIBE through the ESB interface. VIBE compares the information provided on petitions against the D&B data. VIBE then generates a VIBE Scoring Result after comparing the petitioning entity data against an algorithm.
- **DOL** notifies USCIS of the debarred organizations. DOL also publishes a list of

debarred organizations on its public website.[30] The list includes the business name, address, and disbarment period. When DOL determines that an organization has violated the INA, the organization is subject to a mandatory debarment. USCIS cannot approve the petitions filed by the debarred organization during the debarment period. Therefore, upon receiving the DOL debarment request, USCIS places the debarred organizations on a known fraud list until the debarment period expires.

- **DOJ EOIR** notifies USCIS of disciplined immigration practitioners who are currently ineligible to practice immigration law and posts the same information provided to USCIS on its public website.[31] The list contains practitioner name, city and state, and the effective date of discipline. USCIS will place the ineligible practitioners on the known fraud list until reinstated. DOJ EOIR notifies USCIS when the immigration practitioner is reinstated for practice.

2.4 Discuss how accuracy of the data is ensured.

VIBE streamlines the adjudication of certain employment-based immigration petitions by prescreening the data received from the petitioning entity, or the petitioning entity's attorney or accredited representative. The information collected from petitioners is entered into CLAIMS 3, which is sent over to D&B to retrieve data. D&B collects information directly from businesses and business professionals when they participate in online services, such as apply for a D&B D-U-N-S® Number. D&B also collects information offline from business owners and principals, from businesses' creditors, vendors and suppliers, and from public records such as business registrations and bankruptcy filings. D&B provides businesses and business professionals with access to their information within the D&B databases and with an opportunity to correct verified inaccuracies.[32] VIBE uses this data to validate basic information about companies or organizations petitioning to employ certain alien workers. Although USCIS uses D&B to assist with the adjudication of certain employment-based petitions, USCIS does not use commercial information as the sole basis upon which it grants or denies an immigration benefit.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that data discrepancies between D&B and the petitioning entity-supplied information from CLAIMS 3 and the VIBE scoring analysis may produce inaccurate results, which may adversely affect the benefit determination.

---

[30] DOL posts a list of debarred organizations at http://www.dol.gov/whd/immigration/H1BDebarment.htm and http://www.foreignlaborcert.doleta.gov/pdf/Debarment_List_Revisions.pdf.

[31] DOJ posts a list of disciplined practitioners who are currently ineligible to practice immigration law at http://www.justice.gov/eoir/discipline.htm.

[32] *See* D&B Privacy Policy for more information on its privacy practices, *available at* http://www.dnb.com/privacy-policy.html.

Mitigation: USCIS mitigates this risk by using commercial source information for limited purposes. USCIS uses the IIP to verify and corroborate the information provided by the petitioning entity during the immigrant or non-immigrant employment-based benefit petition process. Public source information is only used to verify or identify inconsistencies with information provided by petitioning entity as part of its petition for immigration-related benefits. Although USCIS uses an IIP to assist with the adjudication of certain employment-based petitions, USCIS does not use commercial information as the sole basis upon which it grants or denies an immigration benefit, investigates benefit fraud, or identifies public safety and national security concerns. USCIS trains all users (i.e., USCIS, U.S. Customs and Border Protection (CBP), and DOS) on the appropriate use of commercial and public source information to preserve the data accuracy and integrity of the original information submitted by a petitioning entity.

As noted, VIBE creates the VIBE Scoring Result by using a series of specially designed algorithms and comparing commonalities and differences between USCIS and D&B data. The VIBE scoring result indicates the viability of a petitioning entity based on an algorithm, which includes match confidence, basic company data elements, and eligibility requirements. If the ISO finds contradictory or derogatory information, the ISO issues a RFE or NOID, which allows the petitioning entity to respond to the contradictory or derogatory information. The VIBE score includes a match confidence score, which is a measurement of the level of confidence in the match between the information submitted by the petitioning entity and the information received from the IIP. Information about the D&B matched company provided on the VSR can only be reliable if the petitioning entity has been successfully matched to an entity in D&B's records. The match confidence score is directly related to the overall scoring result.

SCOPS mitigate the risk of maintaining inaccurate information on the known fraud lists during the referral process. SCOPS forwards each known fraud list request to CFDO for review and concurrence with the request form. This process is to reduce the risk of inaccurately identifying a fraudulent case. In addition, CFDO can recommend terminating the entity's known fraud status at any time along with the concurrence of all CFDOs.

Privacy Risk: There is a risk in relying on data obtained from internal and external entities, which may be inaccurate.

Mitigation: When SCOPS receives VIBE known fraud list requests from internal USCIS components and external LEAs, SCOPS reviews each request and determines whether to take any further action or to decline the referral. USCIS will not deny a petition solely based upon information from VIBE without first giving the petitioning entity or applicant the opportunity to respond directly to the agency's concerns. In any case in which USCIS contemplates denial, rescission, or revocation of an immigration benefit based on evidence of fraud, the petitioning entity, attorney, or representative is given an opportunity to review and rebut the evidence. USCIS issues an RFE or NOID if it is necessary to resolve relevant inconsistencies or other

issues that emerge upon review of VIBE-supplied information that are material to the benefit requested.

Privacy Risk: There is a risk that an applicant, requestor or petitioner may unknowingly submit an application, request or petition through a known fraud immigration practitioner, which may have adverse effects on an individual, such as denial of an immigration benefit.

Mitigation: USCIS mitigates this risk by providing the applicant or petitioner with the opportunity to explain and resolve any fraud concerns prior to issuing a final decision. If USCIS determines that a known fraud immigration practitioner is involved in an application, request or petition, USCIS will send an RFE or a NOID directly to the applicant or petitioner. USCIS will not deny an immigration benefit based solely on an applicant or petitioner using a known fraud immigration practitioner. The ISO will make a final decision based on the totality of the circumstances.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

VIBE is used to assist an ISO in providing independent verification of petitioning entity information for immigrant and non-immigrant employment-based petitions. VIBE also incorporates a fraud detection process known as the VIBE known fraud list that enables the ISO to verify if an organization, immigration practitioner, or address is currently a subject of an administrative investigation, is suspended from filing with USCIS, is barred by the DOL or DOJ EOIR, or is the subject of an ongoing criminal investigation. VIBE accelerates the adjudicative vetting process for petitions and enhances the agency's anti-fraud capabilities.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. VIBE is not used to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, U.S. Customs and Border Protection (CBP) personnel.[33] USCIS granted CBP

[33] USCIS granted read-only access to the CBP Officers based on the recommendation from the Office of Inspector General (OIG)'s Report 13-107 "Implementation of L1 Visa Regulations" in August 2013. *See* DHS OFFICE OF INSPECTOR GENERAL, OIG-13-107, IMPLEMENTATION OF L-1 VISA REGULATIONS (2013), *available at* http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-107_Aug13.pdf.

access to VIBE to assist in visa petition processing and to promote program integrity. CBP officers may conduct a VIBE check by entering the approved petition receipt number in VIBE to generate a VSR.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that employees will not use information maintained in VIBE consistent with its original purpose and authority.

Mitigation: USCIS mitigates this risk by limiting the purposes for which USCIS uses the information and by limiting access to VIBE. Consistent with SCOPS's mission to efficiently provide quality services for persons seeking immigration benefits while ensuring the integrity and security of our immigration system and FDNS's mission of detecting, deterring, and combating immigration benefit fraud, USCIS uses the information contained in VIBE to validate the eligibility and viability of the petitioning entity, identify possible benefit fraud or criminal activity related to immigrants and non-immigrants, and identify public safety and national security concerns. The DHS Office of Inspector General (OIG) recommended USCIS grant VIBE access to CBP to assist in visa petition processing and to promote program integrity. CBP officers at northern border Ports of Entry and preclearance locations use VIBE to assist in nonimmigrant petition processing. These uses are consistent with the notice provided to individuals in the Privacy Act Statements on all USCIS forms, this PIA, and corresponding SORNs.

Privacy Risk: There is a risk that derogatory information is incorrectly associated with an individual.

Mitigation: All information obtained by CFDO and reviewed by ISOs is reviewed in accordance with a strict set of internal procedures intended to ensure that actionable derogatory information meets the standards for evidence established by the USCIS Administrative Appeals Office, the DOJ EOIR, and the federal court system.

USCIS incorporates strenuous verification procedures to ensure accuracy of data before an adjudicator makes an immigration benefit decision. These procedures include direct queries of DHS and other government agency databases as well as USCIS ISO interviews with applicants, requestors or petitioners. Public source information is used to verify or identify inconsistencies with information provided by applicants, requestors or petitioners as part of their application, requests and petitions for immigration-related benefits. In any case when USCIS contemplates denial, rescission, or revocation of an immigration benefit based on evidence of fraud, the petitioner or applicant will be given an opportunity to review and rebut the evidence.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

USCIS provides notice prior to the collection of information by publishing this PIA, Alien File, Index, and National File Tracking SORN, Fraud Detection and National Security Records SORN, and the Benefits Information System SORN.[34] USCIS also provides notice on all USCIS applications, requests and petitions at the point of collection through a Privacy Act Statement on the application, request or petition instructions.

In addition to Privacy Act Statements on all USCIS form instructions, USCIS notifies the petitioning entity that information provided may be verified by USCIS. USCIS ISOs may request additional evidence from the petitioning entity during the adjudicatory process and FDNS IOs may verify information by various means, such as conducting interviews during site visits.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

A signature-required release authorization for the relevant benefit request presented to individuals who seek USCIS benefits provides individuals the opportunity to consent. A Privacy Act Statement on the form instructions details the authority for requesting the information and purpose of the information collection. The individual's signature on the form serves as certification that the individual authorizes the release of any information to determine eligibility. Individuals are notified at the point of data collection of the right to decline to provide the required information; however, such action may result in the denial of the benefit request.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may be unaware of how his or her information will be used.

Mitigation: On the Privacy Act Statement in the form instructions, USCIS notifies the individual seeking USCIS benefits that the information he or she provides will be used to determine whether he or she is eligible for the immigration benefit requested. As part of the application, request or petition process, individuals authorize the release of any information from their records that USCIS may need to determine eligibility for the benefit requested.

[34] *See* DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS/USCIS-006 FDNS Records, 77 FR 47411 (Aug. 8, 2012); DHS/USCIS-007 - Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

Privacy Risk: There is a risk that the immigration practitioner is unaware of how his or her information will be used.

Mitigation: An individual appearing as an attorney or accredited representative for a benefit applicant is informed on the form instructions that he or she is subject to the rules of Professional Conduct for Practitioners.[35] Under the rules, information may be disclosed to the public. If FDNS finds that a complaint about criminal conduct has merit, the complaint may also be referred to appropriate investigative or prosecutorial authorities within DOJ or DHS. Additionally, this PIA, DHS/USCIS/PIA-013(a) FDNS PIA,[36] and DHS/USCIS-006 FDNS SORN[37] explain that USCIS gathers information on immigration practitioners that are the subject or associated with a fraud, public safety, or national security concern based on applications or requests submitted on behalf of individuals seeking an immigration benefit.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

USCIS is proposing a 15 year retention schedule for all VIBE records. VIBE will store and maintain VIBE records and known fraud lists indefinitely until a NARA appraisal is completed.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The primary risk associated with retention is that data will be maintained longer than necessary increasing the risk of unauthorized access, use, and loss of data.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the proposed retention period for VIBE is consistent with the Fair Information Practice Principle of retaining PII only for as long as necessary to support the agency's mission. The proposed 15-year retention schedule for VIBE data provides access to information that can be critical to investigating fraud, criminal activity, egregious public safety, or national security concerns for applicants or petitioning entities who may still be receiving immigration benefits.

In addition, if the individual applies for another benefit, retention of the information can eliminate the need for redundant research on concerns that were previously addressed. This approach reduces the likelihood of a duplicate data collection since the investigator may access the previously conducted research. This proposed timeframe also allows SCOPS to ensure that cases that were reviewed and determined to have no nexus to fraud, criminal activity, egregious public safety, or national security concerns are not opened again because old information is recycled.

---

[35] *See* 8 CFR § 292.3
[36] *See* DHS/USCIS/PIA-013(a) FDNS, *available at* www.dhs.gov/privacy.
[37] *See* DHS/USCIS-006 FDNS Records, 77 FR 47411 (Aug. 8, 2012).

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Certain employees at DOS Consular Affairs receive read-only access to VIBE. When reviewing visa applications, DOS has a need for read-only access to VSRs in VIBE. A Memorandum of Agreement (MOA) signed by DOS and DHS on Nov. 18, 2008 governs the VIBE data-sharing agreement between two agencies.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of VIBE data with the DOS is covered by Benefits Information System SORN routine use I, Alien File, Index, and National File Tracking System of Records routine use O, and Fraud Detection and National Security Records SORN routine use I, which permit the sharing of data "for the purpose of assisting in the processing of petitions, requests or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements."[38]

Additionally, the SORNs listed in Section 1.2 allow for the sharing of information stored in VIBE, for law enforcement, national security, and benefit eligibility purposes.

6.3 Does the project place limitations on re-dissemination?

Yes. The project limits re-dissemination to the terms of sharing agreements, including MOAs. The MOA between USCIS and DOS fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination. Methods and controls over dissemination of information are coordinated between USCIS and DOS prior to information sharing. USCIS and DHS are required to obtain consent before producing, transmitting, and copying records for disclosure to a third party unless USCIS and DOS have an agreement or arrangement, memorialized in writing, to authorize such sharing.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

USCIS maintains audit trail logs and uses them to identify transactions performed by external users. DOS users access VIBE through the ESB interface. An interconnectivity agreement exists between VIBE and the ESB. Communication between the ESB and DOS is

[38] *See* DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS/USCIS-006 FDNS Records, 77 FR 47411 (Aug. 8, 2012); DHS/USCIS-007 - Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

covered by a separate interconnectivity agreement.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Sharing can increase the risk of misuse, unauthorized access to, or disclosure of information.

Mitigation: USCIS and DOS conduct electronic sharing of VIBE data over secure government networks. All DOS personnel are trained on the appropriate use and the safeguarding of data. In addition, DOS has policies and procedures in place to prevent the unauthorized dissemination of the information provided by VIBE is prohibited, thereby reducing the risk. Further, any disclosure must be compatible with the purpose for which the information was originally collected and only authorized users with a need-to-know may have access to the information contained in VIBE. As discussed above, VIBE maintains a record of disclosure of VIBE information made with agencies in accordance with the routine use or with which it has an information sharing agreement. A record is kept as system audit trail logs, which are maintained to identify transactions performed by both internal and external users.

Section 7.0 Redress

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

An individual may gain access to his or her USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record the request can be mailed to the following address:

National Records Center

Freedom of Information Act/Privacy Act Program

P. O. Box 648010

Lee's Summit, MO 64064-8010

The information requested may, however, be exempt from disclosure under the Privacy Act because records related to fraud, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations. Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may correct the data maintained by VIBE by following the processes

described in this PIA and associated SORNs. In addition, prior to using commercial, public, and other agency information to render adjudicative decisions, individuals are given an opportunity to refute the derogatory information. Individuals are also afforded appeal and motion opportunities. In the event inaccuracies are noted, VIBE records will be updated.

7.3 How does the project notify individuals about the procedures for correcting their information?

USCIS notifies individuals of the procedures for correcting their information on USCIS forms, the USCIS website, this PIA, and associated SORNs.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an individual may be unaware of his or her ability to make a request to access or correct his or her records in VIBE.

Mitigation: This PIA and associated SORNs notify individuals about how to file a Privacy Act request for records contained in VIBE is provided by this PIA. An individual may request access to information about himself or herself through the Privacy Act or FOIA process, and may also request that his or her information be amended by contacting the National Records Center. The nature of VIBE and the data it collects, processes, and stores is such that it limits the ability of individuals to access or correct their information. However, DHS has exempted VIBE from the notification, access, and amendment provisions of the Privacy Act of 1974 because VIBE contains sensitive information related to possible immigration benefit fraud and national security concerns.[39] Each request for access or correction is individually evaluated.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. USCIS has also established technical and policy safeguards; thereby mitigating privacy risks associated with authorized and unauthorized uses, specifically misuse and inappropriate dissemination of data. Some practices such as the data retention and deletion processes are also automated to ensure compliance. USCIS maintains audit trails to track and identify unauthorized uses of VIBE information. The audit trails include the ability to identify specific records each user accesses. VIBE uses the ESB-Common Services for Auditing.

User access to VIBE is limited to personnel who need the information to perform their job functions. Only users with proper permissions, roles, and security attributes are authorized to

[39] 5 U.S.C. § 552a(k)(2).

access the system. Each user is obligated to sign and adhere to a user access agreement, which outlines the appropriate rules of behavior tailored for VIBE. The system administrator is responsible for granting the appropriate level of access. Furthermore, all employees are properly trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

In addition, USCIS provides a warning banner at all access points to VIBE to inform users of the consequences associated with unauthorized use of information. The banner warns authorized and unauthorized users about the appropriate uses of the system, that VIBE may be monitored for improper use and illicit activity, and the penalties for inappropriate usage and non-compliance.

In keeping with the audit controls and role-based access safeguards established under the DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites PIA,[40] the SCOPS ECN site has a designated site owner, or administrator, responsible for determining the user base and ensuring the site is only used for approved purposes such as internal collaboration and document and workflow management. The site owner ensures that only users with a verifiable need to know have access privileges to the information on the SCOPS ECN site. The SCOPS ECN environment includes a template with a "Sensitive Personally Identifiable Information Allowed" banner at the top of pages approved to manage and share sensitive PII. In addition, the SCOPS ECN site follows the compliance restrictions placed on ECN usage by completing this PIA and the accompanying SORN. SCOPS regularly reviews the information posted to the ECN site, and if inappropriate posting of PII is discovered, SCOPS ensures its immediate removal from the site and reports the posting as a privacy incident.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

USCIS, CBP, and DOS employees are required to complete the annual Computer Security Awareness training and Privacy Awareness training. This training addresses the use of the system and appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). In addition, USCIS requires that all VIBE users receive training in the use of VIBE prior to being approved for access to the system.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

In compliance with federal law and regulations, users receive access to VIBE on a need-to-know basis. This need-to-know is determined by the individual's current job functions. A

[40] *See* DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites PIA, *available at* www.dhs.gov/privacy.

non-DHS user may receive read-only access to the information if he or she has a legitimate need–to-know as validated by his or her supervisor and the system owner, and has successfully completed all personnel security and privacy training requirements.

A user requesting access must complete and submit an ESB Application Access form for VIBE Access. This application requires the user to provide a justification for the level of access requested. The requestor's supervisor, the system owner, and the USCIS Office of the Chief Information Officer will review this request; if approved, the requestor's clearance level is independently confirmed and the user account established.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Sharing agreements between USCIS and other components of DHS, as well as sharing agreements between USCIS or DHS and other agencies, define information sharing procedures for data maintained by SCOPS. Sharing agreements document the requesting agency or component's legal authority to acquire such information, as well as USCIS's permission to share in its use under the legal authority granted by the INA. The program, USCIS Privacy Officer, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, the DHS Office of General Counsel, and the DHS Office of Policy review all sharing agreements through the standardized DHS information sharing and access agreement review process.

Responsible Officials

Donald K. Hawkins

USCIS Privacy Officer

Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security