Privacy Impact Assessment
for the

USCIS Background Vetting Service

March 22, 2010

Contact Point
Gregory Powell
Office of Information Technology (OIT)
United States Citizenship and Immigration Services
(202) 272-7200

Reviewing Officials
Donald Hawkins
Chief Privacy Officer, USCIS
(202) 272-8404

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

Abstract

The United States Citizenship and Immigration Services (USCIS) developed the Background Vetting Service (BVS) to comply with the Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248 which restricts the ability of any U.S. citizen (USC) or lawful permanent resident alien (LPR) who has been convicted of any "specified offense against a minor" from filing certain family-based immigration petitions. Under the BVS, the USCIS will facilitate fingerprint checks of USCs whose principal residence is overseas filing family-based immigration petitions at Department of State (DOS) Overseas Posts against the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Automated Biometric Identification System (IDENT). The information is collected and assembled by DOS. The USCIS BVS does not collect or originate any information but only serves as a conduit to route the information between DOS, US-VISIT, FBI IAFIS, and the USCIS BVS Users. USCIS Conducted this privacy impact assessment (PIA) because BVS checks personally identifiable information (PII) collected by DOS against US-VISIT's IDENT and FBI's IAFIS and returns a status flag back to DOS for their use in the adjudication of the applicable petition.

Overview

Although the authority to adjudicate family-based immigration petitions rests with USCIS, DHS has delegated authority to Department of State, Bureau of Consular Affairs (DOS-CA) to adjudicate certain family-based immigration petitions filed at DOS Overseas Posts by USCs whose principal residence is overseas and who have maintained that residence for at least six months. This delegation of authority is limited to the following petition types: Form I-130, Petition for Alien Relative; Form I-360, Petition for Amerasian, Widow(er), or Special Immigrant; and Form I-600 Petition to Classify Orphan as an Immediate Relative. Under the terms of the delegation of authority, DOS-CA officers may adjudicate such a petition only if the petition is "clearly approvable," acting on the petition is deemed to be in the national interest, or an emergent or humanitarian situation exists.

The Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248 (the Adam Walsh Act) restricts the ability of any USC or LPR who has been convicted of any "specified offense against a minor" as defined by the Act to obtain approval of certain types of immigration petitions including:

- a USC's immediate relative or family-based immigrant petition, or nonimmigrant fiancé(e) petition, and
- an LPR's family-based immigrant petition (LPRs may not file immediate relative or fiancé(e) petitions).

The scope of the BVS includes family-based immigration benefit petitions filed at DOS Overseas Posts by USCs whose principal residence is overseas and who have maintained that residence for at least six months. If the petitioner has been convicted of any "specified offense against a minor," then the DOS-filed petition is no longer "clearly approvable" and must be referred to USCIS.

To enforce this Act for family based petitions filed overseas with DOS-CA (that is to determine if an overseas petitioner has been convicted of a "specified offense against a minor"), the DOS Overseas Post will collect the fingerprints of USC petitioners filing family based immigration petitions. These 10-prints are then checked against the FBI IAFIS[1] and US-VISIT IDENT[2] to determine if the petitioner has committed

[1] For FBI's related privacy documentation, see the IAIFIS and DOJ/FBI Interim Data Sharing Model PIAs at http://foia.fbi.gov/iafis.htm, and http://foia.fbi.gov/idsm.htm, respectively and corresponding SORN for the FBI

a specified offense against a minor. FBI IAFIS and US-VISIT IDENT contain fingerprint matched records which may include criminal history and derogatory information, respectively, that may include "specified offenses against a minor."

As part of the process, USCIS will forward the 10-prints sent by DOS to US-VISIT IDENT and to FBI IAFIS via US-VISIT using an existing connection that US-VISIT maintains with the FBI. FBI IAFIS will return results (e.g. criminal history) to USCIS via US-VISIT. US-VISIT IDENT will return results (e.g., derogatory information) to USCIS via the US-VISIT connection. USCIS will examine the criminal history and derogatory information and determine if a "specified offense against a minor" is included in the criminal history or the derogatory information. The BVS will facilitate the USCIS processing of the criminal history and derogatory information to determine if it contains a "specified offense against a minor." If the criminal history or derogatory information does contain a "specified offense against a minor" the USCIS BVS will send a "Red Status" back to DOS, to advise DOS that the petition is no longer "clearly approvable" and thus should be referred to USCIS. If the criminal history or derogatory information does NOT contain a "specified offense against a minor," the USCIS BVS will send a "Green Status" back to DOS to advise DOS that the petition is "clearly approvable." These flags (Red Status/ Green Status) are sent back to DOS as an input condition into the DOS adjudication of the family based immigration petition filed at the DOS Overseas Post. The "Red Status" indicates to DOS-CA that the petition is "not clearly approvable," and that the consular officer must refer the petition to the appropriate USCIS office for adjudication. When the petition processing is transitioned from DOS-CA to USCIS, the petition and its processing will transfer to a USCIS overseas office which has jurisdiction over the adjudication of the petition, and is no longer within the DOS or BVS process lifecycle. No background information, criminal history, or derogatory information is sent to the DOS for the USC petitioner other than the Red Status or Green Status.

Typical Transaction

USCIS provides the BVS through the USCIS Enterprise Service Bus (ESB), an infrastructure that supports the use of individual services within a Service Oriented Architecture (SOA). The USCIS ESB is a set of commercial off-the-shelf software that provides a standardized infrastructure to connect to multiple systems and services. The following are the process steps of the information processing for BVS:

1. An Overseas Department of State Consular Post collects PII, including biometric information, on behalf of USCIS and maintains it in the Department of State Consular Consolidated Database (DOS-CCD) system.[3]
2. The DOS-CCD system creates a transaction containing the subject identification information and biometric information and delivers it to the USCIS BVS to be forwarded to US-VISIT IDENT and FBI IAFIS via and existing connection to US-VISIT.

Fingerprint Identification Records System (FIRS)(JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410 and associated blanket routine uses at 66 FR 33558 and 70 FR 7513-02) which can be found at http://foia.fbi.gov/firs552.htm .

[2] For DHS US-VISIT's related privacy documentation, see the PIA for the US-VISIT Program for the First Phase of the IOC of Interoperability between the U.S. DHS and the U.S. DOJ at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_phase1ioc.pdf and corresponding SORN for the DHS Automated Biometric Identification System (IDENT), DHS-2007-0027 FR Volume 72, Number 107, Pages 31080-31082 which can be found at http://edocket.access.gpo.gov/2007/07-2781.htm

[3] See U.S. Department of State Privacy Impact Assessment: Consular Consolidated Database, (December 11, 2008).and corresponding System of Records Notice, Visa Records, STATE-39.

3. Both FBI IAFIS and US-VISIT IDENT return identifying information and any information concerning any criminal history or derogatory information of the subject to USCIS BVS via and existing connection to US-VISIT.
    - If no criminal history is found in IAFIS and no derogatory information is found in US-VISIT IDENT, BVS will automatically send a Green Status (e.g., "clearly approvable") to the DOS-CCD system and the DOS-CA officer may therefore proceed with completing the adjudication of the petitions.
    - If a criminal history record is returned by FBI IAFIS or derogatory information is returned by US-VISIT IDENT, the criminal history or derogatory information data is presented to a Background Adjudicator at the USCIS Vermont Service Center Background Check Unit to determine if the petition is "clearly approvable" based on the content of the criminal history or derogatory information. Once a determination is made as to whether the petition is clearly approvable, or not, the appropriate status flag is sent via the BVS to the DOS-CCD system.
4. A copy of the criminal history record or derogatory information, if applicable, returned by FBI IAFIS and US-VISIT and the BVS produced Red Status/Green Status are stored in the USCIS enterprise Citizenship and Immigration Service Centralized Operational Repository (eCISCOR) Operational Data Store (ODS) eCISCOR (outside the system boundary of BVS).[4]

All information related to the USCIS BVS will be transmitted utilizing secure electronic transfer methods (XML over HTTPS) which meets DHS Sensitive Systems Policy Directive 4300A. Although USCIS BVS orchestrates the transmission of data between systems (e.g., DOS-CCD, US-VISIT IDENT, FBI IAFIS, eCISCOR) and authorized users (e.g., Background Adjudicators), BVS itself does not store any data other than an audit log of the transmissions. The derogatory information or the criminal history record returned by US-VISIT IDENT or FBI IAFIS, respectively, and the status flag are not stored within the boundary of the USCIS BVS but rather a copy is transmitted to and stored by USCIS eCISCOR.

[4]See Privacy Impact Assessment for eCISCOR (August 24, 2009) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_eciscor.pdf).

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

USCIS BVS does not collect or originate any information but only serves as a conduit to route the information between DOS, US-VISIT IDENT, FBI IAFIS via an existing connection to US-VISIT, and the USCIS BVS users. The information obtained for background vetting includes biographic, personal identification and biometric data provided at the time of application. The biographic data includes full name, place and date of birth. The identification information includes Social Security number (SSN) and citizenship status. The biometric data includes eye color, hair color, height and weight, race, 10-print fingerprints and the date and time the biometric data were captured. The above data elements will be entered into the DOS-CCD and transmitted to the USCIS BVS. Data returned by FBI IAFIS and US-VISIT IDENT includes personal identification information and any criminal history or derogatory information that exists for the individual being fingerprinted. A copy of the criminal history record returned by FBI IAFIS and a copy of the derogatory information returned by US-VISIT IDENT, for 10-prints processed by BVS and the BVS produced Red Status/Green Status are kept in eCISCOR (outside the system boundary of BVS).

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

USCIS BVS does not collect or originate any information but only serves as the conduit to route information between DOS, US-VISIT IDENT, FBI IAFIS (via US-VISIT), and the USCIS BVS users. The DOS-CCD system creates the transaction containing the subject identification information and biometric information and delivers it to the USCIS BVS to be forwarded to US-VISIT and FBI IAFIS via and existing connection to US-VISIT. FBI IAFIS then returns identifying information and any information concerning any criminal history of the subject to USCIS BVS via an existing connection to US-VISIT. US-VISIT IDENT also returns identifying information and any information concerning any derogatory information of the subject to USCIS BVS via an existing connection to US-VISIT. BVS generates a status flag based on whether or not a criminal history record or derogatory information was returned. If no criminal history or derogatory information is returned, BVS will automatically send a Green Status to the DOS-CCD system. If criminal history or derogatory information is returned, this information is presented to a Background Adjudicator at the USCIS Vermont Service Center Background Check Unit to determine if the petition is "clearly approvable" based on the content of the criminal history and derogatory information. Once a determination is made as to whether the petition is clearly approvable, or not, the appropriate status flag is sent via the BVS to the DOS-CCD system.

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

This information is being collected, used and disseminated in order to determine whether a USC immigration petitioner has criminal convictions that are subject to the Adam Walsh Act.

1.4 How is the information collected?

The information is collected and assembled by DOS. The USCIS BVS does not collect or originate any information but only serves as a conduit to route the information between DOS, US-VISIT IDENT, FBI IAFIS via an existing connection to US-VISIT, and the USCIS BVS users.

1.5 How will the information be checked for accuracy?

It is up to DOS and the USCIS Background Vetting Center to determine the accuracy of the data. This capability is beyond the scope of the USCIS BVS. The BVS monitors transmission to and from its services to catch any network transmission errors. The BVS also validates the data received during a transmission against its defined XML (extensible Markup Language) Schema. XML Schemas are used to define message formats for messages that will be exchanged between systems. XML Schemas are used to ensure that XML messages are 'valid'. It ensures that data that is sent and received follow the designed message formats to avoid receiving and sending data that's not part of the predefined message format.

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

The authority to adjudicate Forms I-130, Petition for Alien Relative, and Forms I-360, Petition for Amerasian, Widow(er), or Special Immigrant (filed by widow(er)s) can be found in 8 CFR 204.1(e)(3). The authority to adjudicate Forms I-600, Petition to Classify Orphan as an Immediate Relative can be found in 8 CFR 204.3(g)(2).

The authority to perform criminal background checks for petitioners can be found in 8 CFR 103.2(e)(1), which states:

(e) Fingerprinting.

(1) General. USCIS regulations in this chapter, including the instructions to benefit applications and petitions, require certain applicants, petitioners, beneficiaries, sponsors, and other individuals to be fingerprinted on Form FD-258, Applicant Card, for the purpose of conducting criminal background checks. On and after December 3, 1997, USCIS will accept Form FD-258, Applicant Card, only if prepared by a USCIS office, a registered State or local law enforcement agency designated by a cooperative agreement with USCIS to provide fingerprinting services (DLEA), a United States consular office at United States embassies and consulates, or a United States military installation abroad.

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

Privacy risks that an adjudication decision could be erroneously made based on inaccuracies in the underlying information (e.g. DOS-CCD and/or FBI-IAFIS) are mitigated in that USCIS BVS only helps determine if a petition filed overseas via DOS is either "clearly approvable" or not. If a petition is erroneously marked NOT "clearly approvable" by BVS a petition will NOT be denied, but rather, will be referred to USCIS for a full review and adjudication under the full USCIS adjudication process.

Any potential privacy risk associated with the unauthorized disclosure of personally identifiable information are mitigated by the almost instantaneous transfer of the data utilizing secure HTTP (HTTPS) followed by the rapid deletion of the record from USCIS BVS systems. The criminal history or derogatory information returned by US-VISIT IDENT or FBI IAFIS is not stored within the boundary of the USCIS BVS but rather a copy transmitted to and stored by USCIS eCISCOR.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The purpose of BVS is to help DOS-CA determine if a family-based immigration petition is "clearly approvable" by having DHS screen the USC petitioners pursuant to 8 CFR 103.2(e)(1). If a "Red Status" is returned by DHS, this will indicate to DOS-CA that the petition is not "clearly approvable," and that the DOS-CA officer must refer the petition to the appropriate USCIS office for adjudication.

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

Data analysis is not part of the functionality of the USCIS BVS. Data produced by the USCIS BVS is limited to the Red or Green Status based on whether or not a Background Check Analyst determined if a "specified offense against a minor" is included in the criminal history or derogatory information returned by FBI IAFIS or US-VISIT IDENT.

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

The USCIS BVS does not use any commercial or publicly available data.

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: Inappropriate use of the information.

Mitigation: User access to the USCIS BVS User Interface will be limited to those who need to perform background adjudication, to determine if a petitioner has committed a specified offense against a minor. The USCIS ESB system administrator will be responsible for granting the appropriate level of access. All USCIS employees will be properly trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

DHS Management Directive System (MD) Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, May 11, 2004, provides guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information in both paper and electronic records (including criminal history data from FBI IAFIS, or derogatory information from US-VISIT IDENT). Additionally, all DHS employees will be required to take annual

privacy awareness and computer security training, which addresses this issue. DHS will also maintain rules of behavior for employees who use DHS systems.

Section 3.0 Retention

3.1 What information is retained?

The USCIS BVS does not retain any information other than the Service's generated transaction audit data. The transaction audit data does not include the 10-print nor does it include any PII data. This logging of transaction audit data is required by the DHS Sensitive Systems Policy Directive 4300A *Section* 5.3 - *Audit Logs Maintained*.

During the processing of a background vetting request, BVS will store the Status flag (Red Status / Green Status) along with a copy of any criminal history or derogatory information returned by FBI IAFIS or US-VISIT IDENT in USCIS eCISCOR. The copy of the FBI criminal history, the US-VISIT IDENT derogatory information, and the Red Status / Green Status determination is kept in eCISCOR. As a decision-aid tool, BVS helps DOS-CA consular officers determine if a family-based immigration petition is "clearly approvable" based on the requirements of the Adam Walsh Act. The rest of the adjudication process takes place within the DOS-CA systems. Copies of data that BVS retrieved from other systems (e.g., FBI IAFIS, US-VISIT IDENT) are kept in eCISCOR until the life cycle of the adjudication process has completed.

3.2 How long is information retained?

The USCIS BVS does not retain any information other than transaction audit data. This data is available online for a period of 180 days. Off site retention of this data is for 7 years. This requirement is per *Section* 5.3 - *Audit Logs Maintained* of the DHS - 4300A which states: "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of 7 years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease."

The copy of the FBI criminal history, the US-VISIT IDENT derogatory information, and the Red Status / Green Status determination is kept in eCISCOR (outside the BVS system boundary) until the life cycle of the adjudication process has been completed. Once the process has completed the data will be discarded, although the audit log record of the transaction will be retained.

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

Not expressly: this is the standard retention period specified by DHS Certification and Accreditation (C&A) policy for system audit data. This requirement is per *Section* 5.3 - *Audit Logs Maintained* of the DHS - 4300A which states "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of seven years as part of

managing records for each system to allow audit information to be placed online for analysis with reasonable ease."

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

Risk: Maintaining personal information for a period longer than necessary to achieve the Adam Walsh enforcement objectives.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the USCIS BVS has the capability to discard the data USCIS BVS stores in eCISCOR, once the petition has been fully processed. This capability is consistent with the concept of retaining PII only for as long as necessary to support the agency's mission.

The data retained beyond the end of the lifecycle for processing the petition is retained solely for the purpose of reconstructing events in the case that unauthorized access is suspected and is not used for any other purpose. The ability to manually review user access patterns after the fact if unauthorized activity is suspected greatly mitigates the possibility of misuse of BVS. This would be done by querying all transactions conducted by the suspected user. This data is stored in the ESB audit tables within the ESB Oracle database which is only accessible by ESB administrators with the appropriate role to read the audit database tables.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

USCIS BVS will send the 10-prints received by DOS-CCD to US-VISIT IDENT and FBI IAFIS. USCIS BVS will store the Status flag (Red Status / Green Status) along with a copy of any derogatory information or criminal history returned by US-VISIT IDENT or FBI IAFIS in eCISCOR.

Only the USCIS BVS users within the USCIS Vermont Service Center Background Adjudication Unit will have access to the data processed by BVS.

Although BVS does not share this information, the 10-print information stored at US-VISIT IDENT and FBI IAFIS is shared as described in Section 4.0 of their respective PIAs (PIA for the US-VISIT Program for the First Phase of the IOC of Interoperability between the U.S. DHS and the U.S. DOJ; FBI PIA IAFIS National Security Enhancements; FBI PIA DOJ/FBI-DHS Interim Data Sharing Model (IDSM). The copy of the criminal history, derogatory information, and the Status flag (Red Status / Green Status) stored in eCISCOR is not shared outside of the background checking process, whatsoever.

4.2 How is the information transmitted or disclosed?

The USCIS BVS system interfaces (e.g., DOS-CCD, US-VISIT IDENT/FBI IAFIS, eCISCOR) transmit data utilizing a FIPS 140-2[5] compliant secure transfer method which meets DHS Sensitive Systems Policy Directive 4300A.

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: Unauthorized access to criminal history or derogatory information stored in eCISCOR after it is stored by USCIS BVS.

Mitigation: User access to criminal history and derogatory information stored in eCISCOR will be limited to only USCIS BVS Users who need the information to perform their job functions - to perform Adam Walsh background check on DOS petitioners.

Access to criminal history or derogatory information stored in eCISCOR will only be made available to be viewed through the USCIS BVS application through USCIS BVS authenticated users. The data will not be made available to general eCISCOR user population.

All USCIS BVS authorized users must authenticate using a user ID and password. DHS policies and procedures are also in place to limit the use of and access to USCIS BVS to the purposes for which it was provided; perform Adam Walsh Act-related background checks on USCs who file family-based immigration petitions with DOS-CA. Computer security concerns are minimized by the fact that the information it not shared, other than to perform Adam Walsh Act-related background check on USCs who file family-based immigration petitions with DOS-CA.

An audit log will be maintained to track all system transactions in USCIS BVS and eCISCOR. The audit log, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access, or destruction.

Although BVS does not share this information, the 10-print information stored at US-VISIT IDENT and FBI IAFIS is shared as described in their respective PIAs and SORNs. The copy of the criminal history, derogatory information, and the status flag (Red Status / Green Status) stored in eCISCOR is not shared outside of this background checking process, whatsoever.

[5] Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2, is a U.S. government computer security standard used to accredit cryptographic modules.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

USCIS BVS will send the 10-prints received by DOS-CCD to US-VISIT IDENT and FBI IAFIS. USCIS BVS will store the status flag (Red Status / Green Status) along with a copy of any derogatory information or criminal history returned by US-VISIT IDENT or FBI IAFIS in eCISCOR.

Although BVS does not share this information, the 10-print information stored at US-VISIT IDENT and IAFIS is shared as described in their respective PIAs and SORNs. The copy of the criminal history, derogatory information, and the status flag (Red Status / Green Status) stored in eCISCOR is not shared outside of the background check process.

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.

Data transmission between DOS, US-VISIT IDENT and FBI IAFIS, as well as the background vetting result (e.g., clearly approvable/Green Status or not clearly approvable/Red Status based on the requirements of the Adam Walsh Act) by USCIS, is authorized by the Adam Walsh Act. The copy of the criminal history or derogatory information stored in eCISCOR is not shared outside of the USCIS background check process. The status flag (Red Status / Green Status) is provided to the DOS as a result of the Adam Walsh Act-related background check request, to determine whether the petition is "clearly approvable."

The authority to perform criminal background checks for petitioners can be found in 8 CFR 103.2(e)(1). The authority to perform this specific type of background check (to determine if a petitioner has been convicted of a "specified offense against a minor") is governed by the Adam Walsh Child Protection and Safety Act of 2006.

The 10-print information stored at US-VISIT IDENT and IAFIS is shared as described in their respective PIAs and SORNs.

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

The USCIS BVS system interfaces (e.g., DOS-CCD, US-VISIT/FBI IAFIS, eCISCOR) transmit data utilizing a FIPS 140-2 compliant secure transfer method which meets DHS Sensitive Systems Policy Directive 4300A.

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

Privacy Risk: The primary privacy risk in external sharing is the sharing of data for purposes that are not in accordance with the stated purpose and use of the original collection.

Mitigation: The 10-print information provided by DOS-CCD for Adam Walsh Check Request and stored at US-VISIT IDENT and IAFIS is shared as described in Sections 4.0 of their respective PIAs. This use aligns with these respective PIAs (PIA for the US-VISIT Program for the First Phase of the IOC of Interoperability between the U.S. DHS and the U.S. DOJ; FBI PIA IAFIS National Security Enhancements; FBI PIA DOJ/FBI-DHS Interim Data Sharing Model (IDSM)).

If future modifications to the BVS system call for additional external sharing of data that passes through BVS, all external sharing arrangements will be consistent with existing routine uses or performed with the consent of the individual whose information is being shared, unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements. These routine uses limit the sharing of information from the system to the stated purpose of the original collection.

Privacy Risk: Inappropriate Use of Personally Identifiable Information (Social Security Number, A-number, etc.)

Mitigation: USCIS provides access to the system only to individuals who have a specific need to know for the purpose of their job. Risks are further mitigated by provisions set forth in MOUs with federal and foreign government agencies. United States government employees must undergo annual computer security awareness training.

Section 6.0 Notice

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

Yes, in addition to this PIA, the data processed by USCIS BVS system is sourced from DOS-CCD, DHS IDENT, and FBI IAFIS provide notice through their respective Systems of Record. Further, USCIS applications contain a Privacy Act statement and a provision by which an applicant authorizes USCIS to release any information received from the applicants as needed to determine their eligibility for immigration and naturalization benefits.

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

No. The data received by USCIS BVS comes from the underlying connected IT systems; DOS-CCD, DHS IDENT, and FBI IAFIS. However, individuals who submit applications for immigration benefits are asked to provide their consent to release the information to assist in the determination of an individual's

eligibility for a benefit. The following is an example of the language found on an immigration benefit application:

YOUR CERTIFICATION: I certify under penalty of perjury under the laws of the United States of America, that the foregoing is true and correct. Furthermore, I authorize the release of any information from my records that U.S. Citizenship and Immigration Service need to determine eligibility for the benefit that I am seeking. Source: Form I-130 (Rev 10/26/05) Y Page 2.

An individual has the right to decline to provide the required information and consent; however, failure to do so may result in the denial of the requested benefit 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?

No. The data received by USCIS BVS comes from the underlying connected IT systems; DOS-CCD, US-VISIT IDENT, and FBI IAFIS. However, a Privacy Act Statement detailing authority and uses of information is presented to the individual on the forms I-130, I-360, and I-600 that the USC would use to file their petition under BVS. These forms also contain a signature certification and authorization to release any information from an individual record that USCIS needs to determine eligibility, including biometric and biographic information. All USCIS applications include a Privacy Act Statement and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…" See the Section 6.2.

Consent is given for any use to determine eligibility, when the individual signs the application. An individual has the right to decline to provide the required information and consent; however, failure to do so may result in the denial of the requested benefit request.

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 stand alone systems that are connected to the USCIS BVS collect personally identifiable information as a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk that an individual may not be fully aware that their information will be used by BVS is associated with this particular collection of information. In order to mitigate this risk, USCIS provides a Privacy Act Statement on its applications. The application also contains a signature certification and authorization to release any information provided by the individual.

Section 7.0 Access, Redress and Correction

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

As a decision aide tool, the USCIS BVS helps DOS-CA consular officers determine if a family-based immigration petition is "clearly approvable" by determining whether the petitioner has ever been

convicted of a "specified offense against a minor" for purposes of the Adam Walsh Act, as indicated in their criminal history record via IAFIS, or derogatory information returned via US-VISIT IDENT. That is all that the USCIS BVS does in this context. The rest of the adjudication process takes place within the DOS-CA systems. The USCIS BVS does not contain any mechanism that would enable individuals to gain access to the BVS copy of their information that was either copied from the origin system of record (e.g., IAFIS, US-VISIT) or derived (e.g., clearly approvable/Green Status or not clearly approvable/Red Status). Rather, individuals may seek access to information provided to USCIS through the means published in the applicable system of records. In order to gain access to one's information stored in the source IT systems, a request for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to them are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his or her account number and/or full name, date and place of birth, and notarized signature, and any other information that may assist USCIS in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, FOIA/PA Request, from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS web site, located at www.uscis.gov.

An individual who would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

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

The underlying connected IT systems are fully responsible for any data that they provide to USCIS BVS. The USCIS BVS is a specialized service and has no mechanisms for generalized updates to its connected systems; DOS-CCD, US-VISIT IDENT and FBI IAFIS.

With regard to a "Red Status" result, individuals will have an opportunity to contest and request the correction of their data that may have resulted in a "Red Status," once the petition is referred to the appropriate USCIS office for adjudication. Since the petition would no longer be "clearly approvable," DOS-CA must refer the petition to USCIS for adjudication. When the petition processing is referred to USCIS, the adjudication of the petition will be completed by the USCIS overseas office which has jurisdiction over the petitioner's overseas place of residence. The processes and procedures for correcting inaccurate or erroneous information, as it then may exist in the petition is documented within the SORN DHS-USCIS-007 - Benefits Information System September 29, 2008 73 FR 56596 (for I-130s, I-360s) and the SORN DHS/USCIS-005 - Inter-Country Adoptions Security June 5, 2007, 72 FR 31086 (for I-600s and I-800s) under the section "Contesting Record Procedures."[6]

6 SORN DHS-USCIS-007 - Benefits Information System September 29, 2008 73 FR 56596 published at http://edocket.access.gpo.gov/2008/E8-22802.htm and SORN DHS/USCIS-005 - Inter-Country Adoptions Security June 5, 2007, 72 FR 31086 published at http://edocket.access.gpo.gov/2007/07-2783.htm.

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

The Privacy Act SORN for the connected system (DOS-CCD, US-VISIT IDENT, FBI IAFIS) provides individuals with guidance regarding the procedures for correcting information. 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?

Petitioners are provided opportunity for redress as discussed above.7.1 and 7.2

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

Risk: The main risk 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 adjudication process to correct information they have provided and to respond to information received from other sources. USCIS does not claim any Privacy Act access and amendment exemptions for this system so individuals may avail themselves to redress and appeals 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?

USCIS personnel and contractors who have received the appropriate security and privacy training will have access to the USCIS BVS User Interface. The primary user groups at USCIS include background vetting officers, supervisors, and support staff. In addition, the ESB Staff and Operations and Maintenance contractors (e.g., the operators) working on developing and supporting the USCIS BVS infrastructure may also have access to the system.

8.2 Will Department contractors have access to the system?

Only to the extent that contractors are used for background vetting responsibilities will contractors have access to the system. This access must be granted on an individual-by-individual basis by the supervisors of the users who request access. In addition, the Operations and Maintenance contractors (e.g., the operators) who support the USCIS BVS infrastructure may also have access to the system.

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

USCIS provides training to all BVS users. This training addresses relevant privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements, etc.). Each USCIS site has the responsibility to ensure that all federal employees and contractors receive the required annual computer security awareness training and Privacy Act training.

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

BVS is being implemented as a Service within the FISMA system USCIS Enterprise Service Bus General Support System (GSS). In March of 2010, the USCIS ESB GSS platform and its services obtained a re-certification with a three year Authority to Operate (ATO) from the USCIS CIO after completing DHS C&A requirements. eCISCOR received a full C&A and was granted an ATO on September 16, 2008 and expires on September 16, 2011. DOS-CCD was granted an ATO on March 1, 2007 and expires on February 28, 2010. DHS US-VISIT's IDENT was granted an ATO on May 10, 2007 and expires on May 9, 2010.

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

The USCIS BVS is provided through the USCIS ESB. The USCIS ESB's full auditing capabilities are implemented and are in use by the USCIS BVS in accordance with the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook. This includes the auditing of any BVS transactions. The USCIS ESB maintains this audit data on the servers in use by the system and these servers have been secured according to standards established by DHS policies. This helps ensure that no unauthorized access occurs on these servers and that the audit data is securely maintained.

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 accessed by USCIS BVS and associated systems, there are inherent security risks, e.g., unauthorized access, use and transmission/sharing.

Mitigation: Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. 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. USCIS BVS and associated systems have a comprehensive audit trail tracking and maintenance function that stores information on who submits each query, when the query was run, what the response was, who received the response, and when the response was received. Data encryption is employed where appropriate to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, USCIS BVS and associated systems comply with DHS and FISMA/NIST security requirements, which provide criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Each time USCIS BVS and associated systems are modified, the security engineers review the proposed changes and if required, perform Security Testing and Evaluation (ST&E) to confirm that the controls work properly. All personnel are required to complete annual online computer security training.

Section 9.0 Technology

9.1 What type of project is the program or system?

The USCIS BVS is a composite service provided through USCIS ESB, an infrastructure that supports the use of individual services within a SOA. The USCIS ESB is a set of commercial off-the-shelf software that provides a standardized infrastructure to connect to multiple systems and services.

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

The USCIS BVS is currently in the development stage, using the USCIS Information Technology Lifecycle Methodology.

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

No. The BVS does not employ technology that raises privacy concerns.

Responsible Officials

Gregory Powell, Office of Information Technology

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security