



APPENDIX A

Administrative Site Visit and Verification Program Load Balancing Utility (ASVVP Load Balancing Utility)

Summary:

FDNS is launching the ASVVP Load Balancing Utility which is a Microsoft Access data form linked to a secure SQL server database to collect receipt data and manage the case selection process. FDNS employees will manually enter the application receipt number, the date the application was adjudicated as “approved,” the validity period of the application, and the beneficiary’s work site address located within the file. Cases subject to review include all applications that FDNS currently conducts an ASVVP site visit and are considered relevant to the ASVVP project mission, by type of form, class preference, and other pertinent criteria.¹

The database will also contain tables that provide geographical connections between USCIS Field Offices and all zip codes throughout the U.S. and protectorates. The ASVVP Load Balancing Utility combines the geographical zip code/Field Office information with the zip code of the Work Site Address to pre-filter the eligible applications into groups based on proximity to a Field Office. Regional managers can then select a Field Office, and the utility will then present the total number of eligible records located within range of the selected Field Office. The regional managers will enter a number representing the estimated work load limit for the selected Field Office and submit a request for randomization. The utility will then randomly select the requested number of applications from the displayed list and provide an exportable workload list for the selected office. Each randomly selected petition will be flagged in the utility so it cannot be selected twice.

The spreadsheets derived from the utility will contain the field office identifier, the receipt number for the application, the approval and validity dates, and the work site address. This information will be attached to an email and sent via secure means (i.e., encrypted) to the Service Center Fraud Detection Operation (CFDO) units² to be utilized by Service Center personnel in pulling the records that are to be entered into FDNS-DS under the existing FDNS-DS PIA.

The expected result of the use of this utility will be a level playing field that affords reasonable workloads to USCIS Field Offices while maintaining as much of the random selection process as possible.

This is a desktop type utility that uses non-sensitive data from recognized sources to

¹ ASVVP site visits are currently conducted on: 1) pre and post adjudication religious worker cases; and 2) approved, post adjudication H-1B (non-immigrant, specialty occupation worker) cases.

² Currently, only the California and Vermont CFDOs process ASVVP cases.



enhance the workload balancing for the entire ASVVP. The overall benefit of this utility will be to enforce the stability and efficiency of the ASVVP.

Data Elements:

Data will include the application receipt number, the date the application was adjudicated as “approved,” the validity period of the application, the beneficiary’s work site address located within the file, and geographical Zip code/Field Office information.

Population:

Cases subject to review under ASVVP.

Privacy Mitigation:

Access to the ASVVP Load Balancing Utility is determined by the FDNS ASVVP program which approves access on an individual basis. User login information is recorded in the data structure and is used to validate access. Unless the user’s login information is validated, neither access to the SQL database nor the Microsoft Access front end is allowed. General users have read only access and there are a small number of manager level users. Manager level users access data based on their location only. The data are of limited scope. Users can only select and/or edit within regional/office profiles that are controlled by rigid filtering. No deletions are permitted except on request to the data managers.



APPENDIX B

Security Checks for Temporary Protected Status (TPS) Applicants

Background:

Pursuant to 8 U.S.C. § 1254a, the Secretary of Homeland Security may designate a foreign country for Temporary Protected Status (TPS) due to conditions in the country that temporarily prevent the country's nationals from returning safely, or in certain circumstances, where the country is unable to handle the return of its nationals adequately. USCIS may grant TPS to eligible nationals of certain countries (or parts of countries), who are already in the United States. Eligible individuals without nationality who last resided in the designated country may also be granted TPS. See DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) for more information on the processing of benefits at USCIS.³

The Secretary may designate a country for TPS due to the following temporary conditions in the country:

- Ongoing armed conflict (such as civil war);
- An environmental disaster (such as earthquake or hurricane) or an epidemic; or
- Other extraordinary and temporary conditions.

During a designated period, individuals who are TPS beneficiaries or who are found preliminarily eligible for TPS upon initial review of their cases (*prima facie* eligible):

- Are not removable from the United States;
- Can obtain an employment authorization document (EAD); and
- May be granted travel authorization.

Once granted TPS, an individual also cannot be detained by DHS on the basis of his or her immigration status in the United States. TPS is a temporary benefit that does not lead to lawful permanent resident status or give any other immigration status. However, registration for TPS does not prevent an applicant from:

- Applying for nonimmigrant status;
- Filing for adjustment of status based on an immigrant petition; and/or
- Applying for any other immigration benefit or protection for which you may be eligible.

TPS designation is time-bound and requires the Secretary to extend designation (re-designate) for a country's TPS status. Re-designation allows USCIS to accept new applications for TPS. Once granted TPS, an individual must re-register during each re-registration period to

³ The CLAIMS 3 PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.



maintain TPS benefits. Please see table below for a full list of countries that have been designated as TPS by the Secretary of Homeland Security and their effective dates.

Designated Country	Most Recent Designation Date	Current Expiration Date	Current Re-Registration Period	Current Initial Registration Period	Employment Authorization Document (EAD) Automatically Extended Through
<u>El Salvador</u>	March 9, 2001	March 9, 2015	May 30, 2013 through July 29, 2013	N/A	March 9, 2014
<u>Haiti</u>	July 23, 2011	July 22, 2014	October 1, 2012 through November 30, 2012	N/A	July 22, 2013
<u>Honduras</u>	January 5, 1999	January 5, 2015	April 3, 2013 through June 3, 2013	N/A	January 5, 2014
<u>Nicaragua</u>	January 5, 1999	January 5, 2015	April 3, 2013 through June 3, 2013	N/A	January 5, 2014
<u>Somalia</u>	September 18, 2012	March 17, 2014	May 1, 2012 through July 2, 2012	May 1, 2012 through October 29, 2012	NO Automatic Extension* *Sufficient time was deemed available to issue new EADs.
<u>Sudan</u>	May 3, 2013	November 2, 2014	January 9, 2013 through March 11, 2013	January 9, 2013 through July 8, 2013	NO Automatic Extension* *Sufficient time was deemed



Designated Country	Most Recent Designation Date	Current Expiration Date	Current Re-Registration Period	Current Initial Registration Period	Employment Authorization Document (EAD) Automatically Extended Through
					available to issue new EADs.
<u>South Sudan</u>	May 3, 2013	November 2, 2014	January 9, 2013 through March 11, 2013	January 9, 2013 through July 8, 2013	NO Automatic Extension* *Sufficient time was deemed available to issue new EADs.
<u>Syria</u>	October 1, 2013	March 31, 2015	June 17, 2013 through August 16, 2013	June 17, 2013 through December 16, 2013	N/A

Applicants for immigration benefits from USCIS, including TPS, receive background and identity checks as part of the adjudication process. Currently, all applicants for TPS receive a biographic check using the Customs and Border Protection’s TECS, as well as a biometric check using the Federal Bureau of Investigation Fingerprint Check. In addition to these checks, USCIS will conduct additional screening on individuals who may be eligible for TPS based off their country of citizenship or to stateless persons who last resided in the designated country. This additional check will be conducted by the Fraud Detection and National Security (FDNS) Division in conjunction with the National Counterterrorism Center (NCTC). FDNS facilitates the additional screening of TPS applicants; however, the Service Center Operations Program (SCOPS) manages the TPS adjudication process.

Screening of TPS Applicants from Designated Countries:

As part of its administration and enforcement of the Immigration and Nationality Act, USCIS reviews TPS applications for “inadmissibilities” under the Immigration and Nationality Act that may affect a TPS applicant’s eligibility for the benefit. For example, USCIS’s review



for inadmissibilities includes national security and terrorism-related inadmissibilities as described in Sections 212(a)(3)(A), (B), or (F), or 237(a)(4) (A) or (B) of the Immigration and Nationality Act.

To support USCIS's identification of terrorism-related inadmissibilities, USCIS is partnering with the NCTC to determine if Terrorism Information exists in TPS applications from designated countries. Terrorism Information is defined as,

(A)... all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information.⁴

Using CLAIMS 3, USCIS will extract TPS applicant data and provide that list to the NCTC via encrypted electronic transmission in accordance with information security standards.⁵ NCTC will analyze the TPS applicant data in conjunction with other data that NCTC holds, such as the Terrorist Identities Datamart Environment (TIDE), to determine if the TPS applicant data constitutes Terrorism Information.⁶ In the event that NCTC identifies Terrorism Information associated with a TPS applicant, USCIS will review all available, relevant information and will adjudicate the application pursuant to USCIS's legal authorities.

Data Elements:

USCIS will provide NCTC with the biographic information derived from TPS applications, such as name, date of birth, country of birth, or other biographic data elements relevant to screening. DHS will not collect, generate, or retain any personally identifiable information beyond that which is collected, generated, or retained during the routine adjudication of TPS applications.

⁴ As defined in 6 USC § 485.

⁵ The DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3), is available at www.dhs.gov.

⁶ TIDE is the central repository of identities information for known and suspected terrorists (KST). TIDE supports the U.S. Government's terrorist screening systems and the Intelligence Community's overall counterterrorism mission. The NCTC developed TIDE as part of the post-9/11 reform of the United States' watchlisting process, which consolidated multiple databases of international terrorist identities. The NCTC can perform batch queries of TIDE and other classified holdings, to determine if Terrorism Information exists for a subject.



Population:

Currently, the only population of individuals that are undergoing this screening are Syrian TPS Applicants. This PIA Appendix will be updated as additional countries are required to have this additional check.

Privacy Mitigation:

DHS and NCTC have entered a letter of intent (LOI) that establishes the terms and conditions of NCTC's access, use, and retention of Syrian TPS information. The LOI limits NCTC's retention of TPS information so that NCTC only retains the information USCIS provides for analysis for as long as required to complete the mission. Under the LOI, NCTC may temporarily retain TPS information until no later than April 30, 2015. The purpose of this extended retention is to enable NCTC to continue to use the Syrian TPS Data in its counterterrorism analysis and to inform DHS of any subsequent terrorism-related concerns that may be identified after NCTC has performed the initial vetting of the Syrian TPS Data. The LOI also requires NCTC to delete the TPS information after it is no longer needed. After April 30, 2015, if the TPS information has not been identified as Terrorism Information, then NCTC will purge the records. If, during the course of the temporary retention period, NCTC identifies TPS information that is Terrorism Information, NCTC may retain, use, and disseminate the information consistent with its authorities.

The LOI also features protections against unauthorized dissemination of TPS information. Pursuant to the LOI, NCTC may disseminate Syrian TPS Data identified as Terrorism Information consistent with its authorities without the need for DHS approval, provided such dissemination is to other appropriate federal departments and agencies with counterterrorism responsibilities for counterterrorism purposes. NCTC may not otherwise disseminate Syrian TPS Data absent written permission from DHS, including review and approval by USCIS, the DHS Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and Policy Office.



APPENDIX C

Form I-854, *Inter-Agency Alien Witness and Informant Record*

Summary:

The USCIS Fraud Detection and National Security Directorate (FDNS) Law Enforcement Support Operation (LESO) Branch adjudicates benefit applications and ancillary benefits, coordinates with USCIS field offices for various programs, generates notional documents for undercover operations, and provides advice on law enforcement and intelligence agency-sponsored immigration benefits programs. One of the roles of FDNS is to provide immigration assistance to law enforcement entities. The S nonimmigrant program falls under this responsibility.

Congress established the S nonimmigrant program as part of the Violent Crime Control Act of 1994.⁷ This program provides a nonimmigrant status for alien witnesses or informants who meet the requirements and are sponsored by law enforcement entities. The alien witness or informant may be eligible to receive S nonimmigrant status by: (1) providing critical and reliable information concerning a criminal or terrorist origination or enterprise; (2) willing to supply such information to law enforcement entities or court; or (3) showing his or her presence in the U.S. is essential to the success of a criminal investigation or prosecution of an individual involved in a criminal or terrorist organization or enterprise. Law enforcement agencies (LEA) use USCIS Form I-854, *Inter-Agency Alien Witness and Informant Record*, to bring alien witnesses and informants to the United States in an S nonimmigrant classification.

Form I-854 consists of two parts: the I-854A and I-854B. Form I-854A is used to place an alien in S nonimmigrant status while Form I-854B is used to recommend the alien for adjustment of status.⁸ Both parts are submitted by the sponsoring LEA to request inadmissibility waivers for the alien and as a supporting document when submitting an application for permanent residence on behalf of a witness or informant. The form is circulated through several entities for review and concurrence before reaching USCIS, starting with the sponsoring LEA, the alien, a United States Attorney's office, U.S. Department of State, and U.S. Department of Justice, Criminal Division, before finally reaching USCIS. Each of these entities provides its signatory endorsement, which is required under 8 CFR Part 214.2(t)(4). The concurrence of each entity is required in order to waive any inadmissibility. When Form I-854A reaches USCIS, the form and supporting documentation are presented to the Associate Director of FDNS and a decision is made to approve or deny the request. Upon USCIS approval of the status, Form I-854A and all documentation provided in support of the Form are placed in the alien's

⁷ Pub. L. No. 103-322 § 13003, 108 Stat. 1796, 2024-26 (codified at 8 U.S.C. 1101(a)(15)(S) (2012)).

⁸ The Form I-854B step occurs after the individual has completed the terms and conditions of his or her S classification.



respective Alien File (A-File). USCIS provides an approval letter to the LEA and the applicant may choose to submit an I-765, *Application for Employment Authorization*.

FDNS reviews the Form I-854B in support of Form I-485, *Application to Register Permanent Residence or Adjust Status*. USCIS will then process the Form I-485 pursuant to USCIS adjudicator's standard operating procedures.

Data Elements:

USCIS may collect personally identifiable information (PII) about the alien witness or informant and the alien witness or informant's derivative family members in connection with a Form I-854 filing, including: name, alias, address, A-Number, I-94 number, current location of alien, marital status, date of birth, place of birth, nationality, occupation, date of last entry into the U.S., criminal history, FBI number, Social Security Number, passport number, travel document number, S-Visa number, country of issuance of passport or travel document, expiration date of passport or travel document, place of last entry, date of last entry into the U.S., current immigration status (if changing status), class of admission, country of origin, gender, and signatures. The Form only collects this information for alien witnesses and informants sponsored by a law enforcement entity, as well as any family members that may be deriving the benefit.

USCIS may collect PII about the LEA in connection with a Form I-854 filing, including: agent name, requesting LEA, address, e-mail address, phone number, fax number, and signature.

Population:

The form is used by LEAs to bring an alien witness and informants to the United States in an S nonimmigrant classification, change an existing nonimmigrant classification to an S classification or adjust an S nonimmigrant classification to lawful permanent resident status.

When completing the Form I-854A, LEAs must request one of the following classifications:

- (1) S-5 nonimmigrant classification: For an alien who possessed and is willing to provide to the requesting LEA critical, reliable information on a criminal organization and who otherwise qualifies under section 101(a)(15)(s) of the Immigration and Nationality Act (Act) and 8 CFR 214.2(t).
- (2) S-6 nonimmigrant classification: For an alien who possessed and is willing to provide information on a terrorist organization, who will be or is placed in danger as a result, and is eligible for an award under section 36(a) of the State Department Basic Authorities Act of 1956, 22 USC 2708(a), and who otherwise qualifies under section 101(a)(15)(S) of the Act and 8 CFR 214.2(t).



Qualifying relatives (spouse, married and unmarried sons and daughters, and parents) of the principal alien witness and informant may be included in a request for the S nonimmigrant classification.

Privacy Mitigation:

USCIS only collects a limited amount of PII in order to adjudicate this form. The information collected is pursuant to 8 U.S.C. § 1101(a)(15)(S). The information is only used for the purposes outlined on the form instructions.

USCIS ensures that the PII that is collected is accurate and complete as best practical, by collecting information directly from the applicant and/or LEA.

After USCIS processes this form, USCIS places it directly into the individual's A-File. USCIS controls the subject's A-File for 100 years from the date of birth, and then transfers the files to National Archives and Records Administration (NARA) for permanent retention pursuant to the approved retention schedule [N1-566-08-11]. The A-File is the only place USCIS retains the form.



APPENDIX D

Fraudulent Document Recognition Training

Summary:

The mission of U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directorate's (FDNS) is to determine whether individuals or organizations filing for immigration benefits pose a threat to national security, public safety, or the integrity of the nation's legal immigration system. FDNS supports USCIS's mission by enhancing USCIS's effectiveness and efficiency in detecting and removing known and suspected fraud from the application process, thus promoting the efficient processing of legitimate applications and petitions.

FDNS facilitates the Fraudulent Document Recognition Training to detect and deter fraud by recognizing fraudulent immigration documents as well as detecting impostors. This course trains USCIS personnel on how to identify types of counterfeit identification documents commonly used by terrorists, identification theft offenders, and illegal immigrants. Topics include how to identify immigration documents, specifically Permanent Resident Cards and Employment Authorization Documents (EAD), common document security features, photocopy examination of altered genuine documents, as well as a review on impostor detection.

The purpose of this Fraudulent Document Recognition Training course is to educate and enhance the FDNS employee's ability to identify and differentiate between genuine, counterfeit, and altered documents. The training allows FDNS personnel to determine what fraudulent documents look like and understand how fraudulent documents relate to immigration benefit fraud, issues of terrorism, and other national security issues. During the course of the training, the facilitator provides examples of both genuine and counterfeit documents to distinguish the difference between fraudulent documents and valid documents that have failing or worn features.

USCIS provides Fraudulent Document Recognition Training to USCIS personnel only; USCIS does not use a virtual training environment for this training. FDNS holds this training course in a classroom setting at a secured USCIS facility. The training consists of a PowerPoint presentation covering detection and examination of Permanent Resident Cards and EADs. Instructors share real immigration documentation obtained through fraud investigations or the administrative process to review security features of genuine, counterfeit, and altered documentation. However, there is no handout and students must return all training materials at the end of the training session. The PowerPoint is stored on the FDNS internal drive and the immigration documents are stored in a secured locked room. These training materials are restricted to those with a valid need-to-know.

FDNS will retain this presentation indefinitely and update it as appropriate to include new versions of cards and new fraud techniques employed by aliens to circumvent regulation.



Data Elements:

The training presentation and immigration documents may contain real and fraudulent information about individuals. Personally identifiable information (PII) from the Permanent Resident Card, EAD card, and photocopied documents may include: the individual's name, address, Social Security Number, A-Number, date of birth, receipt filing number, photograph, country of birth, admission code, financial information, employment history, and education history.

Population:

Individuals who submitted fraudulent and altered documents to USCIS.

Privacy Mitigation:

FDNS provides Fraudulent Document Recognition Training to USCIS personnel with a need-to-know for training purposes. To prevent the risk of disclosing more information than necessary, FDNS minimizes the use of PII by removing unnecessary or irrelevant content from training materials that are not aligned with the objective of the training goals.

The electronic PowerPoint will be used as a part of this training. Access to the Fraudulent Document Recognition Training is restricted to employees with a valid need-to-know. The instructor will only use government-issued equipment to store and access this training. FDNS stores this presentation on an internal drive that is not accessible to users outside FDNS. FDNS will maintain security controls for any relevant materials.

FDNS stores the official physical records in a locked compartment and will not leave the records unattended. FDNS will store these records in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room where a guard and card reader controls access. FDNS collects all original, fraudulent, or photocopied document examples provided during training at the end of the training session and stores them securely.



APPENDIX E

Southeast Region Immigration Services Officer Fraud Referral Intake Log

(SER ADJ Fraud Referral Intake Log)

Summary:

FDNS created the *SER ADJ Fraud Referral Intake Log* to capture and track all incoming fraud referrals from U.S. Citizenship and Immigration Services (USCIS) Immigration Services Officers (ISO).

Southeast Region (SER) ISOs document suspected fraud and forward the file to USCIS Fraud Detection and National Security Directorate (FDNS) after a supervisor approves a case for further inquiry. FDNS documents all incoming fraud referrals from ISOs in the *SER ADJ Fraud Referral Intake Log* spreadsheet and creates a record in FDNS Data System (FDNS-DS).⁹

FDNS reviews the referral for completeness and will either accept or decline the referral. If declined, the FDNS-DS record is “closed” and FDNS returns the Fraud Referral Sheet (FRS) to the referring ISO with an explanation of why FDNS declined the referral. If accepted, FDNS designates the case as accepted in FDNS-DS, conducts research and investigation, and refers prosecutable cases to Immigration Customs and Enforcement (ICE) officers.

Maintaining the *SER ADJ Fraud Referral Intake Log* allows FDNS to:

(1) Report Statistics

FDNS Immigration Officers (IO) use the information in the intake log to generate workflow production reports. Each FDNS office manually generates reports and each office captures these reports differently. The intake log allows FDNS offices to report the required numbers with consistency across the region.

(2) Conduct Training

FDNS IOs are responsible for training ISOs on how to refer actionable fraud cases and known fraud patterns and trends. The *SER ADJ Fraud Referral Intake Log* captures the reason FDNS declined a fraud referral, which assists FDNS to identify individual and group training needs.

(3) Complete the FDNS survey

SER FDNS requires all referrals returned to ISOs with findings must have a five question survey attached for ISOs to complete and return to FDNS. Capturing this

⁹ For more information on FDNS-DS, see DHS/USCIS/PIA-013, Fraud Detection and National Security Data System (FDNS-DS), available at www.dhs.gov/privacy.



data on the *SER ADJ Fraud Referral Intake Log* will assist FDNS to determine where the surveys were sent and if a response was received. It also allows FDNS to reach out to the ISO directly to request a completed copy of the survey.

(4) Meet ISO Period Performance Appraisals

Supervisory ISOs request the data from the *SER ADJ Fraud Referral Intake Log* for individual ISO fraud referral counts.

Data Elements:

This log maintains information related to the referral, and actions taken by FDNS and ISOs. Data may include:

Referral Information

- Date of fraud referral
- ISO First Name
- ISO Last Name
- Receipt Number

FDNS Action

- Date created in FDNS-DS
- FDNS-DS Number
- Whether the referral was accepted or declined
 - If declined, the reason it was declined
- FDNS findings

ISO Action

- ISO decision on petition/application
- Date ISO issued a Notice to Appear (if applicable)

Population:

Cases referred by ISOs to FDNS for fraud.

Privacy Mitigation:

Only FDNS personnel with a need-to-know may access the *SER ADJ Fraud Referral Intake Log*. Further, FDNS maintains the intake log on the shared drive with restricted access, and user login and password controls are in place to monitor usage. In addition, USCIS FDNS provides training to all individuals who will be using the log to confirm proper handling of the information that is maintained. Finally, all USCIS employees are required to complete annual



**Homeland
Security**

privacy training, which trains employees on the appropriate handling, use, and dissemination of personally identifiable information.



APPENDIX F

Overseas Verifications

Background:

Overseas Verification (OV) is the verification of events, education, and work experience that occurred in a foreign country or the authentication of documents or information that originated overseas and relate to an individual's application or petition for immigration benefits. USCIS conducts OVs as part of the administrative investigation process.

The USCIS office responsible for administrative investigations is USCIS Fraud Detection and National Security Directorate (FDNS). FDNS performs administrative investigations to produce information that USCIS Adjudications Immigration Services Officers (ISO) may use to determine an individual's eligibility for an immigration benefit. FDNS ensures its administrative investigations are narrowly tailored to verify relationships that are the basis for an individual to receive an immigration benefit; to identify violations of the Immigration and Nationality Act; and to identify other grounds of admissibility or removability.

FDNS Immigration Officers (IO) receive written fraud, national security, and criminal referrals from Adjudications ISOs. FDNS IOs may also receive referrals or Requests for Assistance (RFA) from law enforcement partners, RFAs from other USCIS Directorates and Program Offices, or tip letters from the public. A FDNS IO performs systems checks and research on the subject of the referral. Then, the FDNS IO determines whether to take any further action or decline the referral. If the FDNS IO determines an administrative investigation is necessary, he or she performs further checks to verify information provided on, and in support of, applications and petitions.

A FDNS IO pursues an OV after exhausting all domestic resources, such as research in government and commercial databases, public record research, file reviews, telephone calls, site visits, interviews of witnesses, requests for evidence, and internal RFAs. To initiate the OV process, a FDNS IO completes and uploads an Overseas Verification Request (OVR) into the FDNS Data System (FDNS-DS) and selects the appropriate receiving Overseas Office (USCIS or Department of State (DOS)¹⁰). FDNS-DS then sends an email to the designated Overseas Office to begin the OV. A USCIS or DOS employee working at an Overseas Office (Overseas Officer) conducts the verification of information or documents, including the verification of events, education, and work experience or the authentication of documents that originated overseas. Verification activities include:

- Phone, fax, e-mail, or internet verifications;

¹⁰ USCIS does not have offices in every country worldwide. DOS assists with Overseas Verifications when USCIS does not have an office in a particular country.



- Primary document examination and comparison against local repositories and databases;
- Targeted interviews;
- Consultation with other USCIS offices, DHS components, or DOS employees;
- Consultation with foreign governments;
- Diplomatic notes; and
- Administrative site visits.

In order to verify information associated with an application or petition, the Overseas Officer may contact:

- The individual;
- Third parties with knowledge about the case including joint sponsors or other persons associated with the filing;
- Educational, financial, and governmental institutions;
- Places of employment;
- Religious establishments; and
- Medical facilities.

Once the Overseas Officer has taken all necessary steps to verify the document or information, he or she will input the necessary information into FDNS-DS by completing a Report of Overseas Verification (ROV) template. The ROV must detail the nature of the OV, who conducted the OV, how the OV was conducted, and the findings of the OV. A supervisor will review the ROV prior to returning to the requesting officer. After approval from the supervisor, the Overseas Officer will upload the approved ROV and supporting documents to FDNS-DS. The Overseas Officer then sends an email via FDNS-DS to the domestic officer with the requested information.

Information Collected:

The information collected and retained in FDNS-DS as a result of an OV varies depending on the reason for completing the Overseas Verification. For example, an officer may suspect that an applicant's birth certificate is altered. Therefore, the officer would request for the Overseas Officer to investigate the authenticity of the applicant's birth certificate. Appropriate supporting documentation may include a certified copy of the birth certificate from the foreign entity or a letter indicating that the birth certificate in question was altered. The Overseas Officer verifies the supporting documentation that was received through the case.



Population:

USCIS applicants and petitioners who have submitted information to USCIS to receive an immigration benefit. In some cases, USCIS may not be able to verify documents or information domestically and may need to conduct an administrative investigation or verification overseas.

Privacy Mitigation:

There is a risk that USCIS may disclose information about certain applicants who are designated as special protected classes when conducting an OVR.¹¹ USCIS employees and contractors are required to complete the annual Privacy Awareness Training, which identifies how to safeguard documentation, as well as identify the criminal and civil penalties associated with the unauthorized disclosure of this information. In addition, employees are also given training on special protected classes and how their information should be safeguarded and protected from disclosure.

There is also a risk that USCIS may collect more information than necessary or collect information on the wrong person, as part of an investigation. USCIS mitigates this risk by training employees to narrowly tailor OVRs and ensure the correct information is associated with the request and ROV. Additionally, Overseas Officers only seek to verify items that the FDNS IO is requesting in the OVR. For example, if an FDNS IO requests verification on the legitimacy of a birth certificate, the Overseas Officer will conduct an investigation to confirm its legitimacy.

¹¹ The following federal laws and regulations restrict disclosure to third parties for special protected classes: (1) 8 CFR § 208.6 for refugees and asylum benefit seekers; (2) 8 U.S.C. § 1367 for VAWA benefit seekers; (3) 8 CFR § 246 for LIFE benefit seekers; (4) 8 CFR § 244 for TPS benefit seekers; and, (5) 8 U.S.C. § 1160 for SAW benefit seekers.



APPENDIX G

FDNS Tip Reporting Process

Background:

USCIS FDNS has a growing need for innovative ways to receive and evaluate information from the public and from other governmental entities concerning suspected fraudulent activities in order to effectively anticipate and reduce the impact of immigration fraud.

Currently, there is no clear avenue for the public to report suspected immigration benefit fraud to USCIS. When contacting the USCIS National Customer Service Center (NCSC) to report fraud, individuals are directed to call the U.S. Immigration and Customs Enforcement (ICE) hotline, the U.S. Customs and Border Protection (CBP) phone number, or to visit ICE and CBP webpages. The ICE Law Enforcement Support Center (LESC) previously reviewed the tips and forwarded those that may involve immigration benefit fraud to the USCIS Vermont Service Center (VSC) FDNS Office for further review, routing, and any action the local office deemed necessary. This often resulted in multiple entities having to handle and re-route misdirected correspondences causing unnecessary delays in the processing of time-sensitive information. In addition, there is no mechanism for the public to electronically submit information related to fraudulent activities directly to USCIS.

To actively engage the public in combating immigration benefit fraud, USCIS FDNS created a centralized process for the public to directly report suspected immigration benefit fraud to USCIS. This further aligns with USCIS' strategic goal to strengthen the security and integrity of the immigration system.

USCIS FDNS Tip Reporting Process:

Headquarters FDNS (HQFDNS) has created a mechanism that will centralize the process and identify USCIS as the point of contact for the public and other government agencies to report immigration benefit related tips. The USCIS public website and the NCSC now provide the public and other government agencies (OGAs) with a USCIS email address they can use in order to report tips of alleged fraud.

Individuals are now able to submit a tip to USCIS directly by emailing Reportfraudtips@uscis.dhs.gov or by visiting www.uscis.gov, where a link to the mailbox is provided. The webpage lists suggested fields the reporter should include that FDNS has deemed useful when processing the tip. The list serves merely as a suggestion, the reporter can include as much or as little information as they wish. Furthermore, USCIS collects information from the reporter on a voluntary basis.

Upon receiving a tip, HQFDNS is responsible for logging, vetting, tracking, analyzing the tips received to determine the quantity and quality of information received, and the potential



for successful outcomes. The vetting process, including a search of government systems to identify fraud leads or obtain additional identifying information, determines whether or not the tip is actionable. HQFDNS also assesses the veracity of the tip during the vetting process. If HQFDNS deems the tip actionable, HQFDNS forwards the appropriate office having jurisdiction over the individual (e.g., FDNS Division in the respective field office, Service Center, Asylum or RAIO Office) for investigation.

FDNS documents the tip according to currently established policies, procedures, and practices including the Fraud Standard Operation Procedures (SOP) and the FDNS-DS User's Guide. FDNS documents the query on a designated Enterprise Collaboration Network (ECN) site and the Fraud Detection and National Security-Data System (FDNS-DS).¹² Access to the ECN site and the fraud tip mailbox is limited to individuals assigned to process the emails for distribution to the FDNS Division in the field office responsible for processing the tip. HQFDNS will also use the information to develop reports and track trends or patterns. FDNS logs results of tips that are not actionable on the ECN site and are not forwarded to the respective field office. A copy of each tip is stored in the email archive (.pst) files as well as in the ECN for 15 years in accordance to the NARA Retention Schedule noted in the FDNS PIA dated July 30, 2012.

Information Collected:

USCIS collects fraud tips on a voluntary basis. The type of information collected for each case varies but may include:

- The type of tip being reported (e.g., marriage or employer fraud);
- Whether or not the tip was previously reported to another agency;
- Name of the business or person allegedly committing the fraud;
- Identifying information for the individual/company allegedly committing the fraud to include name, email, phone number, address, nationality, aliases, A-number, and/or date of birth
- Contact information of the person reporting the fraud including full name, email, phone number, and address.
- Any further information the person wishes to provide regarding the tip.

¹² In addition to FDNS-DS, FDNS uses an unclassified SharePoint Services-based repository to manage internal policy and operational documents, content, and reports. Role-based access is granted for officers with a need to know. The repository provides a secure environment to facilitate collaboration among HQFDNS personnel and between HQFDNS and its field officers. The data are protected using security safeguards established by DHS in the DHS/ALL/PIA-037 - DHS SharePoint and Collaboration Sites, available at www.dhs.gov/privacy.



HQFDNS enters fraud tips into FDNS-DS and the ECN site, which are accessible only to authorized employees. If FDNS deems a case inactionable, it is documented on the ECN site, but not entered into FDNS-DS.

HQFDNS employees are also responsible for forwarding the tips to the appropriate USCIS Office (Field Office, Service Center, Asylum or RAIO Office) having jurisdiction over the Subject or pending applications/petitions identified in the tips or other external agencies.

Population:

Any individuals or entities, reported by the general public or OGAs, as well as individuals suspected of committing immigration fraud.

Privacy Risks & Mitigations:

Privacy Risk: Because tips are reports of alleged illegal or otherwise suspicious activities, FDNS will not contact the reported individuals to verify their information. There is a risk that information provided about an individual in a tip may not be accurate because the information is provided by a third party and not the individual himself or herself.

Mitigation: During the course of an investigation into the tip, FDNS uses a variety of resources (government and open sources, as described in the PIA) to determine the accuracy and reliability of the tip information, including in some cases by conducting an interview with the subject of the tip. FDNS always investigates and verifies tips before USCIS uses the information as the basis for an adverse action against an individual.

Privacy Risk: There is a risk that USCIS may retain the tip information for longer than necessary.

Mitigation: USCIS retains the information in accordance with the NARA-approved retention schedule. USCIS retains FDNS-DS records for 15 years from the date of the last interaction between FDNS personnel and the individual, no matter the determination. FDNS retains this information because the information received regarding a case may not be actionable at the time of receipt; however, it may become pertinent at a later date. (e.g., Marriage fraud tip received after USCIS grants LPR status may not be actionable at the time of receipt but can be further investigated at the time the applicant attempts to remove conditions or naturalize).