Privacy Impact Assessment
for the

U. S. Customs and Border Protection

Electronic Secured Adjudication Forms Environment (e-SAFE)

DHS/CBP/PIA-057

March 11, 2019

Contact Point
Keri Brady
Admissibility Review Office
Office of Field Operations
(571) 468-1816

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) is tasked with determining the admissibility of all individuals seeking admission into the United States. For non-immigrants seeking admission into the United States, CBP is automating the collection of information from visa-exempt citizens of Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands who are eligible to apply for temporary and permanent waivers of inadmissibility through the creation of the Electronic Secured Adjudication Forms Environment (e-SAFE). CBP is conducting this Privacy Impact Assessment (PIA) because waiver applicants will now be able to submit information electronically as part of the waiver application process, and because CBP collects, maintains, and disseminates personally identifiable information to vet inadmissible non-immigrants applying for a waiver.

Overview

U.S. Customs and Border Protection (CBP) is tasked with safeguarding America's borders, while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel. To facilitate lawful travel, CBP ensures lawful entry of all travelers seeking admission to the United States. All persons arriving at a port of entry (POE) to the United States are subject to inspection by CBP officers. Upon arrival, CBP officers will process all travelers in accordance with applicable laws.[1] Aliens seeking to lawfully enter into the United States must establish their admissibility to the satisfaction of the CBP officer.

Admissibility is determined by the CBP officer at a U.S. POE in accordance with applicable immigration laws. The Immigration and Nationality Act sets forth grounds for inadmissibility.[2] The general categories of inadmissibility include health, criminal activity, national security, public charge, lack of labor certification (if required), fraud or misrepresentation, prior removals, unlawful presence in the United States, and several miscellaneous categories. For certain grounds of inadmissibility, it may be possible for a person to obtain a waiver of that inadmissibility. In some cases, exceptions are written into the law and no waiver is required to overcome the inadmissibility because the inadmissibility does not apply if the individual meets the exception. Examples include exceptions for aliens who have been battered, abused or subjected to extreme cruelty, who are victims of severe forms of trafficking, and who are minors.

However, most individuals who are seeking admission as non-immigrants, but are inadmissible, can file a request for a waiver of inadmissibility. Many travelers seeking admission as non-immigrants will apply for waivers as part of the visa issuance process. Visa-exempt citizen of Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands who

[1] Additional information regarding the inspection process is located in the Code of Federal Regulations, *see, e.g.* 8 CFR 235 Inspection of Persons Applying for Admission.
[2] Grounds of inadmissibility are found in the Immigration and Nationality Act (INA) § 212(a).

are ineligible to enter the United States due to a ground of inadmissibility must apply for a waiver of ineligibility to CBP's Admissibility Review Office (ARO).

The ARO is CBP's centralized office to render decisions regarding the adjudication of waivers for previously inadmissible, visa-exempt citizens of Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands who complete Form I-192, Form I-212, and Form I-824:

- Form I-192 Application for Advance Permission to Enter as Nonimmigrant,[3] is submitted at ports of entry by inadmissible nonimmigrant aliens already in possession of appropriate documents.[4]
- Form I-212 Application for Permission to Reapply for Admission into the United States after Deportation or Removal, is for a particular inadmissible immigrant and nonimmigrant population that is seeking permission to reapply for admission into the United States (also known as "consent to reapply")[5] after he or she has been excluded, deported, or removed from the United States[6] or had been unlawfully present in the United States for an aggregate period of more than one year, and subsequently entered or attempted to reenter the United States without being admitted.
- Form I-824[7] Application for Action on an Approved Application or Petition is used to request a duplicate approval on an approved application or petition for Forms I-192 and I-212, in cases where an applicant has lost a copy of their original waiver.

Ninety-seven to ninety-eight percent (97%-98%) of nonimmigrants who submit these forms are Canadian citizens. The remaining two to three percent of nonimmigrants who submit these forms are from Palau, Federated States of Micronesia, and the Republic of the Marshall Islands.

CBP intends to begin the e-SAFE as a pilot program in mid-2019. Electronic applications will be able to be submitted only at e-SAFE designated POEs and preclearance locations which initially will be Buffalo, NY; Toronto International Airport Preclearance, Toronto, Canada; and Blaine, Washington. Applicants who are applying at these locations will be able to use e-SAFE during the pilot period. Expansion of the availability of electronic filing via e-SAFE to all waiver-processing POEs and preclearance locations in Canada is expected to begin after successful

[3] The form I-192 is owned by U.S. Citizenship and Immigration Services (USCIS) and available electronically at www.uscis.gov. This form may also be used to apply for T nonimmigrant status and for U nonimmigrants status; however, CBP does not adjudicate T and U nonimmigrant status. T and U nonimmigrant statuses are adjudicated by USCIS.
[4] CBP can grant discretionary relief pursuant to § 212(d)(3)(A) of the INA.
[5] Per Section 212(a)(9) of the INA.
[6] Pursuant to section 212 (a)(9) as stipulated in 8 CFR section 212.2 or 212(d)(3)(A).
[7] Application for Action on an Approved Application or Petition, which allows an applicant to obtain a copy of the decision of their Form I-192 or I-212 application if they become lost/stolen or damaged.

completion of the pilot. e-SAFE pilot POEs will continue to accept paper applications. Applicants who opt for electronic filing during the pilot or at a POE where e-SAFE is available will need to go to an e-SAFE-enabled POE for processing.

Current Paper Process

A visa-exempt individual from Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands who apply for admission at a CBP POE and is deemed inadmissible may apply for a waiver of inadmissibility. Currently, an individual seeking a waiver of inadmissibility must download Forms I-192 or I-212 from the USCIS or CBP websites and manually complete the forms. The applicant must print the completed form, and physically provide the form in-person, as well as some or all of the following additional information, to a CBP officer at a POE for review:

1. Evidence of Citizenship;
2. Completed, signed Forms I-192 or I-212;
3. A properly executed Form G-28, Notice of Entry of Appearance as Attorney or Accredited Representative, if applicant has retained an attorney or an accredited representative for this specific application;
4. Form G-325A[8] completed and signed;
5. A copy of any criminal record or an official letter from the court of jurisdiction stating the reason why a copy of the record is not available;
6. A verified criminal record or evidence of the lack thereof (typically from the Royal Canadian Mounted Police (RCMP)) dated and properly endorsed within 15 months of submission of an application.
7. A statement in applicant's own words, signed by the applicant, explaining the circumstances of each arrest, conviction, and sentence or fine imposed. In addition, the applicant may submit any evidence or explanation of reformation of character or rehabilitation such as counseling or rehabilitation programs completed, current employment, marital status, community service, etc., or any other information he or she believe will strengthen his or her request;
8. If the applicant is inadmissible for one of the health-related grounds identified in the INA, e.g., drug user or addict, he or she must provide evidence of treatment/rehabilitation. Such evidence shall include, but may not be limited to, the following: a recent drug test; credible, verifiable evidence related to rehabilitative history; statement from the applicant making

[8] Form G-325A is a supplemental form that USCIS is retiring and it will no longer be needed with the new revised Form I-192 in the new process.

clear his or her commitment to refrain from unlawful use of controlled substances, credible, verifiable evidence outlining subject's program for substitution therapy/treatment and/or continued care relative to his or her drug use/addiction if allowed to enter the United States; and

9. If the applicant has been found inadmissible under section 212(a)(9)(B) of the INA (unlawfully present in the United States) he or she must submit detailed information regarding:
    a. Current foreign employment;
    b. Previous U.S. employment;
    c. Family members presently living in the United States;
    d. Past and current United States and/or foreign business investments; and
    e. All ties he or she has to present foreign country/residence.

Under the current process, applicants submit the above information in-person to a CBP officer at the POE where they are fingerprinted. The CBP officer verifies that all documents have been provided and properly filled out. If information is missing, the applicant is required to provide the missing or additionally needed information to submit a completed application at the POE. The CBP officer then collects the application filing fee and either captures the applicant's fingerprints electronically or on a fingerprint card. CBP officers at the POE bundle the applications and ship the physical documents and forms to the ARO for adjudication.

Adjudicators at ARO manually input limited biographic information from the waiver applications into the Targeting Framework (TF), a module in the Automated Targeting System (ATS).[9] The ARO uses ATS/TF as a case management system and only inputs information needed to identify and manage the adjudication process including applicant name, date of birth, mailing address, Alien Number, date of application, and date of receipt by ARO.

The ARO adjudicator reviews the application and adjudicates it, if possible. If the application is not complete or ARO needs additional information, ARO sends a request to the alien on Form I-72 (Request for Evidence) for additional informational needed to adjudicate the application. The applicant has 87 days from the issuance date of the I-72 to provide the requested information to the ARO. When all information is present, ARO adjudicates the case and renders a decision. The decision (approval/denial) is mailed to the applicant address of record. Approval

[9] *See* DHS/CBP/PIA-006 Customs and Border Protection Automated Targeting System (ATS) PIA (August 3, 2007), and subsequent updates, *available at* www.dhs.gov/privacy.

letters are shown to CBP officers when the applicant is crossing the border, as evidence of approved waivers.[10]

e-SAFE

To streamline waiver processing and reduce the administrative burden on CBP officers at the POE, CBP has developed e-SAFE to allow visa-exempt individual who would normally apply for a waiver in paper at the POE to apply for a waiver of inadmissibility online (www.e-safe.cbp.dhs.gov). Applicants will still be allowed to submit a paper application at the POE if they do not wish to use the online e-SAFE application, consistent with current regulations. CBP is using e-SAFE to automate the collection, vetting, adjudication, and dissemination of waiver requests and information provided on waiver applications. e-SAFE is a commercial-off-the-shelf product provided by Salesforce and customized to meet CBP needs. e-SAFE is available via a public-facing website and collects the same biographic information currently collected from the paper forms.

e-SAFE Pilot Launch

CBP intends to begin e-SAFE as a pilot program in mid-2019. Electronic applications will only be able to be processed at POEs and preclearance locations in Buffalo, NY; Toronto International Airport Preclearance, Toronto, Canada; and Blaine, Washington. Applicants that indicate they will be applying at these locations will be encouraged to use e-SAFE during the pilot period. Expansion of electronic filing via e-SAFE to all waiver-processing POEs and preclearance locations in Canada is expected to begin after successful completion of the pilot.

e-SAFE Identity Verification and Secure Login at LOGIN.CBP.GOV

e-SAFE will rely on LOGIN.CBP.GOV[11] and identity authentication process authenticate applicants who seek to apply for a waiver. LOGIN.CBP.GOV verifies the authenticity of users looking to access the e-SAFE to apply for waiver of inadmissibility by using a User ID or email address for account creation. LOGIN.CBP.GOV account creation collects biographic and contact information and uses two-factor authentication, sending a temporary, single-use security code to a phone via voice or text to allow a user to log-in. LOGIN.CBP.GOV subsequently shares the user's phone number and email address with the overall e-SAFE system.

LOGIN.CBP.GOV account login access will collect the following information from applicants in order to create a user profile:

[10] In the event that ARO grants a waiver, applicants receive an approved Form I-194 for the I-192 applications or a Form I-272 for the I-212 applications, which they can present to a CBP officer at a POE. CBP officers can manually verify the waiver within CBP systems.
[11] LOGIN.CBP.GOV is not the same as the General Services Administration www.login.gov; rather, it is user authentication functionality through the Salesforce platform.

- E-mail address (also serves as User ID);
- Password; and
- Phone number (for two-factor authentication).

Inadmissible visa-exempt individuals who would normally apply for a waiver in paper at the POE seeking to apply through e-SAFE must create an account by first entering their e-mail address, which will become the applicant's User ID. LOGIN.CBP.GOV automatically sends a link to that applicant's email account, who then must follow the link to verify that the email address is correct. The applicant is then prompted to create a password and enter a phone number. Once entered, LOGIN.CBP.GOV sends a security code via text or voice call to the applicant's phone. The applicant then enters the security code into LOGIN.CBP.GOV to verify his or her identity. After the applicant's identity is verified, LOGIN.CBP.GOV sends an email with a 16-character personal key, which will allow the applicant to verify the account in case of a lost phone or forgotten password.

After successfully logging into e-SAFE, the applicant may complete the necessary Forms (I-192, I-212, or I-824) for which he or she is applying and upload the required documentation needed for adjudication.

e-SAFE Application Processing

Applicants who seek to apply for a waiver after creating an e-SAFE account will login and choose the forms (I-192, I-212, or I-824) they want to fill out. e-SAFE will list step-by-step instructions for each section of the form and walk the applicant through the steps to help the applicant avoids missteps and fill out the form correctly. e-SAFE will ensure that correct supporting documents are uploaded and will not allow the applicant to move from one section to the next until the section is completed and the appropriate supporting documents are provided. e-SAFE will also provide a visual map on the application so the applicant knows the sections that are completed and what is left to be completed. After completing the application and uploading all required supporting documents, the applicant will pay the required fee and tentatively choose the POE where he or she intends to complete the biometric portion of the application.

The required documentation remains the same whether submitting a waiver via e-SAFE or through the paper process; however, e-SAFE has system-level data accuracy checks to ensure that all needed documents are uploaded and that dates are valid to ensure the application is complete before electronic submission and payment. e-SAFE will issue the applicant a unique application identification number that the applicant can print and bring to the POE when he or she reports to the POE for biometric capture and document validation. CBP officers at the POE will continue to review documents to ensure they are originals and are not altered or counterfeit. All documentation

will be stored in the Unified Passenger Module (UPAX), a module of the Automated Targeting System (ATS)[12] for adjudication by the ARO. Biometrics will be stored in CBP's secondary processing application and then sent to the Automated Biometric Identification System (IDENT).[13]

As with the paper process, the automated application may be completed by the applicant or by a third party such as a friend, relative, travel industry professional, or an immigration attorney. Attorneys or accredited representatives must submit a G-28 when filing an application on behalf on a client. However, the applicant must sign the form online before submission. Additionally, the applicant is responsible for the application and supporting documentation that is submitted on his or her behalf. When a waiver applicant has filed, paid, and submitted the application online, the applicant will receive an electronic receipt acknowledging proof of payment of the application and informing the applicant that he or she has 45 days to report to a POE to provide biometrics (fingerprint) to complete the application. If CBP needs additional information to process an application, CBP will electronically send a Request for Evidence (I-72) to the applicant's account where the applicant will receive an email to check his or her e-SAFE account due to a change in his or her application status.

Pay.gov

After completing the application, e-SAFE will redirect the applicant to the Department of Treasury's Pay.gov[14] to pay the application-processing fee. As an e-SAFE interface Pay.gov will electronically update e-SAFE when a payment is made and will generate a receipt that the applicant can print as proof of payment. Once the applicant has paid and submitted the application, the applicant is no longer able to make changes to the application, except to change his or her address, e-mail, and telephone number or to respond to a request from CBP for additional information to process the application.

Biometric Capture and Adjudication

Once the fee is paid, e-SAFE will direct the applicant to a list of CBP POEs (and preclearance locations, when applicable) where the applicant needs to report to provide his or her biometrics required to complete the waiver application. At the POE, a CBP officer will take the applicant's biometrics and will electronically submit the application to the ARO for adjudication.

---

[12] *See* DHS/CBP/PIA-006 Customs and Border Protection Automated Targeting System (ATS) PIA (August 3, 2007), and subsequent updates, *available at* www.dhs.gov/privacy.
[13] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), and associated appendices, *available at* www.dhs.gov/privacy.
[14] *See* Treasury Financial Management Service Pay.gov *available at* http://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm.

At the POE, CBP officers use the e3 Biometrics Module[15] to collect the ten-print fingerprints for enrollment in IDENT.[16] CBP uses IDENT as the central DHS-wide system for the storage and processing of biometric data. IDENT stores and processes biometric data and links biometrics with biographic information to establish and verify identities. Applicant biometrics are transferred to IDENT to create an encounter that generates a unique encounter identification (EID) number. A unique Fingerprint Identification Number is assigned to that individual's fingerprints and is used to group all the encounters that biometrically matched to the individual. DHS and the Federal Bureau of Investigation have established interoperability between IDENT and the Automated Fingerprint Identification System (IAFIS) / Next Generation Identification (NGI) fingerprint databases.[17] Biometrics captured for e-SAFE applications processing will reside in IDENT consistent with the records retention for all passport control inspections.

Continuous Vetting and Targeting

Information collected through e-SAFE, including incomplete and not submitted applications, will be used by CBP for vetting and targeting purposes. As with in-person applications for waivers, CBP treats incomplete and not submitted applications as passport control inspections. ARO will use UPAX, a module of ATS, to vet applicants for security concerns and admissibility. UPAX allows ARO to vet applicant traveler information against other information available in ATS and apply risk-based rules developed from CBP officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other Government agencies. Specifically, the UPAX functionality unifies multiple possible match results from multiple source systems; reduces record duplication and streamlines the review process; standardizes the backend components under the CBP Target Technical Architecture to ensure consistency and improve maintainability and reusability; standardizes the entity resolution algorithms across all match results, providing improved consistency and maintainability as algorithm improvements are made and applied across the system; consolidates the front-end risk assessment components of legacy

[15] *See* DHS/CBP/PIA-012 CBP EID/IDENT Portal (e3) (July 25, 2012), *available at* www.dhs.gov/privacy. The e3 Biometric Module provides the interface to IDENT. The Biometrics Module allows CBP officers to uniquely identify or verify the identity of the individuals they encounter by capturing the apprehended individual's photograph and fingerprints and transmitting them in real-time to IDENT. IDENT searches for possible matches among the repository of fingerprint images in the database. Query results are returned to the e3 Biometric Module. IDENT either matches the fingerprint image to a previously encountered individual's scanned fingerprint or enrolls the fingerprint image in its database by assigning a Fingerprint Identification Number (FIN) since the individual had no biometric records stored in any of the databases. IDENT is the sole repository for the fingerprint image, but the FIN is sent back to the e3 Biometric Module along with any biographic information associated with that fingerprint. The CBP Officer would then compare the query results with the previous encounter records, and look at recidivism to determine if the subject meets a threshold set for a particular enforcement action.

[16] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), and associated appendices, *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

[17] *See* Department of Justice, Federal Bureau of Investigation Privacy Impact Assessments *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

ATS-Passenger module with the case management capabilities of the ATS-Targeting Framework (ATS-TF) under one user interface; and consolidates the query results across multiple source systems into an integrated view, including ATS-TF[18] that eliminates the need for analysts to log into separate systems as they conduct their research.

In addition to making an adjudication determination, CBP will use applicant information for targeting purposes to gain insights on applicant populations and potentially make unknown connections. CBP will store applicant information for vetting for the initial waiver application and will continuously vet applicant information as long as the waiver is valid and the applicant was admitted to the United States for six months before the expiry date of the waiver. CBP uses ATS to recurrently vet the information against various CBP holdings, including customs, immigration, and terrorism-related information. In the event the application information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS System of Records Notice (SORN)[19] (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Application Adjudication

When CBP makes a decision about a submitted application, e-SAFE will generate an email to the applicant prompting the applicant to login into his or her e-SAFE account to check his or her application status. Applicants will also receive an email if their section 212(d)(3)(A) waiver is revoked for any reason.

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?

CBP is establishing e-SAFE under the authority granted INA §§ 212(d)(3)(A)(ii), 212(a)(9)(A) or (C) and title 8 of the Code of Federal Regulations (CFR), section 212.4. The 212(d)(3)(A) waiver allows inadmissible visa exempt nonimmigrants from Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands to apply for advance permission to temporarily enter the United States.

CBP has the discretionary authority to temporarily or permanently waive certain grounds of inadmissibility.[20] INA sections 212(a)(9)(A) or (C) and 8 CFR 212.2 prescribed relief for

[18] ATS-TF continues to exist as a separate module/sub-system within ATS, but UPAX provides the ability to create and manage TF events via the UPAX interface, which can be opened through the ATS-TF application.
[19] *See* DHS/CBP-006 Automated Targeting System (May 22, 2012) 77 FR 30297, *available at* www.dhs.gov/system-records-notices-sorns.
[20] CBP/ARO delegation of waiver authority is found in paragraph II.B.5 in DHS Delegation Order Number: 7010.3, issued on May 11, 2006.

eligible aliens who have been deported from the United States and need to apply for permission to reapply "consent to reapply" to reenter the United States. Section 103 of the INA and 8 CFR 2.1 authorize the Secretary of the Department of Homeland Security (DHS) to administer and enforce the INA and other laws relating to the immigration and naturalization of aliens, and to establish such authority as he or she deems necessary for carrying out his/her authority. Various provisions of the INA and corresponding regulations place limits on the conditions of aliens' entry. *See*, *e.g.*, INA §§ 215(a), 235; 8 CFR 235.1.

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

DHS/USCIS/CBP/ICE-001 Alien File, Index, and National File Tracking System of Records, which covers the collection, use, and storage of the Form I-192, Form I-212, Form I-824 and supplemental documents stored in an individual applicants' A-File. The A-Files contain official record material about each individual for whom DHS has created a record under the INA such as: Naturalization certificates; various documents and attachments (e.g., birth and marriage certificates); applications, petitions, and requests for immigration determinations or agency action under the immigration and nationality laws; reports of arrests and investigations; statements; other reports; records of proceedings before or filings made with the U.S. immigration courts and any administrative or federal district court or court of appeal.[21]

SORN coverage is provided by the DHS/CBP-011 TECS, which allows for the collection of information to determine the admissibility of individuals into the United States.[22]

Additional SORN coverage is provided by DHS/CBP-006 Automated Targeting System, which contains information on vetting admissibility and on admissibility determinations.[23]

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

Yes. CBP developed e-SAFE using the Salesforce platform. e-SAFE is part of the CBP deployment of Salesforce, known as the Customer Relationship Management Tool (C2RMT), which received its Authorization to Operate on March 7, 2018. C2RMT/Salesforce will host and deliver information technology applications that meet e-SAFE needs. Salesforce will be used as a Platform as a Service (PaaS) and as a Software as a Service (SaaS). Salesforce has an approved

[21] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, (September 18, 2017) 82 FR 43556, www.dhs.gov/system-records-notices-sorns.
[22] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008) 73 FR 77778, *available at* www.dhs.gov/system-records-notices-sorns.
[23] *See* DHS/CBP-006 Automated Targeting System (May 22, 2012) 77 FR 30297, *available at* www.dhs.gov/system-records-notices-sorns.

Federal Risk and Authorization Management Program (FedRAMP) and is authorized on the CBP Technical Reference Model (TRM).

As a CBP IT application, e-SAFE will be optimized for use on tablets and mobile devices to improve the user experience.

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

No. ARO staff is working with the CBP Records Office to establish a NARA record and retention schedule for e-SAFE. CBP proposes the following schedule that applies to records replicated on the unclassified and classified networks:

CBP will retain information submitted as part of the e-SAFE website for 5 years after the CBP Admissibility Review Office (ARO) has rendered the final decision, which matches the 5 year maximum validity period of an approved waiver. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 17-year retention period (generally 5 years active, 12 years archived) to active law enforcement lookout records will be matched by CBP to enforcement activities, investigations, or cases, including e-SAFE applications. This retention schedule also applies to incomplete and not submitted applications, for which the retention period begins after the last account activity.

Once the information is archived, the number of officials with access to it will be further limited. Data linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including e-SAFE applications that are denied, will remain accessible for the life of the law enforcement activities to which they are related.

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.

Yes. The e-SAFE program is covered by the PRA. USCIS owns the three immigration forms that ARO uses to processes waiver requests:

- Form I-192 Application for Advance Permission to Enter as a Nonimmigrant – OMB No: 1615-0017. USCIS uses this form to address inadmissibility of individuals seeking T (Victims of Severe Forms of Trafficking in Persons) and U (Victims of Criminal Activity) status under 8 CFR 212.16, 8 CFR 212.17, and 8 CFR 214.14, to apply for permission to enter the United States. The form determines whether the individual should be admitted to the United States temporarily despite the inadmissibility. For T and U applicants, if the waiver is approved, this will allow the T or U applicant to enter the United States, or, if the

T or U applicant is already in the United States, allows the applicant to stay in the United States and receive T or U nonimmigrant status. CBP uses this form to grant temporary permission under INA section 212(d)(3)(A)(ii) and 8 CFR 212.4 to certain inadmissible nonimmigrants who are not required to obtain a visa or are already in possession of the appropriate documents but who wish to enter the United States through a U.S. Port-of-Entry (POE).

- Form I-212 Application for Permission to Re-apply for Admission into the United States After Deportation or Removal – OMB No. 1615-0018. An alien who is inadmissible under section 212(a)(9)(A) or (C) of the Immigration and Nationality Act (INA) files Form I-212 to obtain "consent to reapply for admission" that is required before the alien can lawfully return to the United States. "Consent to reapply" is also called "permission to reapply." At a POE, CBP uses the information provided to find derogatory information not previously divulged or to rule out false matches and facilitate adjudication.
- Form I-824 Action on an Approved Application or Petition – OMB No. 1615-0044. Applicants use Form I-824 to file an action for the approved underlying application or petition when the petitioner/applicant either changes his or her nonimmigrant or immigrant status or needs a new action by USCIS or Department of State (DOS), which is different form that originally requested. Applicants also use the form to request a duplicate approval notice from USCIS or CBP of a petition or application previously approved.

Section 2.0 Characterization of the Information

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

e-SAFE permits applicants to electronically submit the same biographic information for inadmissibility waiver applications that CBP currently collects manually via paper applications.

All waiver applicants are required to submit the following information in e-SAFE, consistent with the data fields published on the paper Form I-192, I-212, and I-824:

- Full name;
- Place of birth;
- Date of birth;
- Sex;
- Race;
- Ethnicity;

- Address(es);
- Country of residence;
- E-mail address;
- Photograph;
- Parents' name, date of birth, and place of birth;
- Spouse's name;
- Employment history;
- Occupation;
- Telephone number(s) (fixed line and mobile phone);
- Country of citizenship;
- Alien registration number (if applicable);
- Passport information;
- Criminal history;
- Biometric data (such as fingerprints);
- Records payment information; and
- Basic biographic information about an attorney or other third party that completed application.

e-SAFE account login access will collect the following information from applicants in order to create a user profile:

- IP addresses;
- E-mail address (also serves as User ID);
- Password; and
- Phone number (for two-factor authentication).

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

e-SAFE collects information primarily from the applicant or his or her representative. Inadmissible visa-exempt individuals who would normally apply for a waiver in paper at the POE would apply for a waiver to enter the United States in e-SAFE by submitting their application via

a secure website. Applicants, or their representative, submit all application information directly. Applicants also provide biometrics in-person at a POE.

CBP may rely on other law enforcement or national security information to determine if discretionary relief will be granted and if additional admissibility concerns may be applicable.

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

No. e-SAFE does not use commercial sources or publicly available data, however CBP users may incorporate public source (e.g., Internet) information obtained for reference or incorporation into operational and analytical reports and/or projects within UPAX.

2.4 Discuss how accuracy of the data is ensured.

The individual applicant or his or her designee/representative submits the information directly to CBP through e-SAFE. Click-through windows and other advisory notices will be provided during the application process for the applicants to acknowledge, read, and understand the required information and e-SAFE privacy policy. The individual applicant is required to certify, under penalty of perjury, that the information he or she provides through e-SAFE is accurate. During the application process, e-SAFE will not allow the applicant to move to the final application page before all the required information is provided. CBP officers at the POEs will check the applicant's information for accuracy when the applicant presents him or herself at the POE to complete the biometric portion of the application. A CBP officer will compare the applicant's biographic and passport information to information submitted in e-SAFE for identity confirmation and accuracy. Additionally, personnel in the ARO will contact the applicant if they need any additional information or to verify information provided.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Because applicants have limited ability to change information once submitted, they may be unable to update application if they have additional information or more accurate information to provide.

Mitigation: Minor changes such as updating a phone number or address can be made by an applicant without requiring a new application. To complete minor changes, the applicant can sign back into his or her e-SAFE account. Significant changes such as a name change, or a change in the answers pertaining to eligibility, require a new application or an Application for Action on an Approved Application or Petition (Form I-824). This is necessary to protect the identity and information of the applicant by ensuring that updates are not made in e-SAFE by someone other

than the applicant or someone authorized to represent the applicant. A new application mitigates the chances that unwanted and/or inaccurate changes are made by someone other than the applicant.

Privacy Risk: There is a privacy risk that eligibility determinations about the waiver will be based on inaccurate information.

Mitigation: This risk is mitigated in several ways; first, direct submission of the information from the source, i.e., applicant, or authorized third parties who have permission from the applicant is presumed to be more accurate. Next, new submissions after prior adjudicated applications will be electronically grouped together, which means the submissions of information by the applicant or authorized third party when the waiver expires helps ensure that the information remains more current and therefore, more accurate. Further, if the application is denied because of a deficiency in his or her information (e.g., failure to provide required information); the applicant has the opportunity to correct the information or resolve the issue by filing Notice of Appeal or Motion. The initial denial may be reversed and the applicant may receive a favorable decision if he or she corrects the deficiency.

Privacy Risk: There is a risk that an e-SAFE applicant status may change prior to his or her travel.

Mitigation: e-SAFE status can change at any time. However, this risk is partially mitigated through the notification of individuals via email as soon as their status changes. CBP vets e-SAFE applications in UPAX, a module of ATS,[24] and other selected security and law enforcement databases such as TECS.[25] CBP may also vet e-SAFE applications against security and law enforcement databases at other federal agencies to increase CBP's ability to determine whether the applicant poses a security risk to the United States. The results of this vetting may support CBP's initial assessment of whether the applicant admission to the United States poses a law enforcement or security risk and whether there may be issues, which may require separate consideration. The applicant must receive a final adjudicative decision regarding discretionary relief prior to seeking entry to the United States.

The e-SAFE system will continuously query/vet application information against law enforcement databases. In instances where CBP discovers a violation that violates the term of the section 212(d)(3)(A) waiver, the waiver will be revoked and the individual will be notified via email to login into e-SAFE account to check the status of their waiver.

[24] *See* DHS/CBP/PIA-006 Customs and Border Protection Automated Targeting System (ATS) PIA, August 3, 2007, and subsequent updates, *available at* www.dhs.gov/privacy.
[25] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing PIA, December 22, 2010, *available at* www.dhs.gov/privacy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The primary use of the information collected in e-SAFE is for ARO to determine if an applicant can be granted a waiver of inadmissibility. In order to determine if a waiver is appropriate ARO will:

1. Use UPAX to vet and to determine whether the individual poses no risk to the security of the United States and if the applicant's reason for being inadmissible can be waived under INA § 212(d)(3)(A).
2. Vet the applicant's information against appropriate systems, such as the Terrorist Screening Database (TSDB) biographic records, Interpol lost and stolen passport records, and the Department of State's lost and stolen passport records, and visa revocations, to determine whether the applicant may require additional review.
3. Archive incomplete application (incomplete application, non-submitted application) within the applicant's e-SAFE "account" for internal CBP management reporting.
4. Communicate with the applicant via the e-SAFE.
5. Verify information on the e-SAFE application during biometric appointment by CBP Officers at POEs.

The information from applications may also be used in conjunction with targeting rules and for other national security purposes.

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. e-SAFE does not analyze any data in the database for purposes of discovering or locating a predictive pattern or an anomaly. e-SAFE collects IP addresses, reviews name matching and vets the information using existing DHS IT systems. CBP will examine the application information by vetting the applicant's data through TECS and other appropriate systems such as the Automated Targeting System.

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

Online web access to e-SAFE will be available to CBP personnel only. However, the information collected by and maintained in e-SAFE may be shared with all component agencies

within DHS on a need to know basis consistent with the component's mission. The information may also be provided to other Federal Partners. Access to e-SAFE information within CBP systems is role-based consistent with the mission of the component and the user's need to know in the performance of his or her official duties.

DHS counterterrorism, law enforcement, and public security communities will be provided with information about suspected or known violators of the law and other persons of concern uncovered via e-SAFE in a timely manner. CBP may share the e-SAFE applicant's PII and vetting results with other components within DHS when there is a need to know in accordance with their official responsibilities, including collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information will be accessed and misused because CBP employees and contractors have access to applicants' information in the e-SAFE system.

Mitigation: In order to become an authorized internal user, personnel must successfully complete privacy training and hold a full background investigation clearance. An internal user must also have a job-related requirement to access the specific information. Additionally, because e-SAFE will use some aspects of the TECS IT platform, all internal users of the e-SAFE system are required to complete and pass an annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy as they are presented. An internal user must pass the test scenarios to retain access to TECS and affiliated TECS IT platform and the training is regularly updated.

To further mitigate the risk of misuse of information by DHS employees and contractors with access to e-SAFE, access to data in e-SAFE is controlled through passwords and restrictive rules pertaining to user rights. Internal users are limited to roles that define authorized use of the system. Management oversight is in place to ensure appropriate assignment of roles and access to information.

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.

CBP will provide notice to the individual at the time of the electronic collection on the website via a Privacy Notice. If an individual has asked a third party to enter the information, the third party is provided the notice and is required to obtain the consent of the individual before entering the information. A Privacy Notice will be provided to the applicants in real time during the applicant's use of e-SAFE. Appropriate notice regarding the data to be collected and the requirement to attest to the accuracy of the data will be included in the information provided via the e-SAFE website. Outreach for e-SAFE will start in early 2019, and will continue to take place throughout CBP components and the selected POEs and preclearance pilot locations. Once operational, CBP officers will inform inadmissible aliens of the option to submit forms electronically through e-SAFE and information will be available on the CBP website.

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

To apply and obtain a valid waiver of inadmissibility to enter the United States, information requested must be provided pursuant to applicable statutes.[26] An applicant who declines to provide information necessary to complete an e-SAFE application will not be able to submit the application until the applicant has provided the required information. The only legitimate means of declining to provide the subject information is to choose not to apply for a waiver of inadmissibility to travel to the United States.

Individuals do not have the right to consent to particular uses of the information. Individuals may decide whether or not they will submit the required information in order to apply for a waiver to travel to the United States. Once an individual submits the data for e-SAFE purposes, he or she cannot exert control over the use of that data, aside from his or her ability to amend specific data elements by accessing his or her account and submitting these data elements.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that they can apply for a waiver through e-SAFE.

Mitigation: Adequate notice and disclaimer information, including the consequences of not providing requested information will be given to applicants and consent will be obtained before

[26] Immigration and Nationality Act Section 212(d)(3)(A)(ii), 8 CFR 212.4.

any information is collected. Individuals who are unaware of the program will be notified to apply via e-SAFE. Furthermore, CBP will establish a website and sustain an information campaign to inform and assist travelers with the system.

Privacy Risk: There is a risk that individuals will not know that CBP retains information from non-submitted and incomplete applications.

Mitigation: This risk is partially mitigated. CBP provides notice that CBP will retain any information entered through e-SAFE CBP via the Privacy Notice on the e-SAFE website and this PIA. e-SAFE has an auto-save feature which will save the application after every section before moving on to the next section. Therefore, e-SAFE will retain any information entered as part of all applications, including incomplete, abandoned, or unpaid applications.

Section 5.0 Data Retention by the project

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

e-SAFE retains information actively for 5 years and in archives for 12 additional years. This includes complete and incomplete applications. The information submitted in e-SAFE is retained to vet prospective travelers seeking to enter the United States. CBP continuously vets information for the life of the waiver, 5 years, and 6 years after if applicant was admitted into the United States. Information will be kept in archives for 12 years to allow retrieval of the information for law enforcement and investigatory purposes.

For information that is included in an individual's official A-File, records are retained permanently, consistent with the A-File SORN. The official A-File record may take three possible forms: (1) records contained within the paper A-File; (2) records contained within the electronic record from Enterprise Document Management System[27] or USCIS Electronic Immigration System;[28] or (3) a combination of paper and electronic records and supporting documentation. A-File records are maintained in accordance with N1-566-08-11. DHS/USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that information will be kept in e-SAFE for longer periods than necessary.

[27] *See* DHS/USCIS/PIA-003(b) Integrated Digitization Document Management Program, *available at* www.dhs.gov/privacy.
[28] *See* DHS/USCIS/PIA-056 USCIS Electronic Immigration System, and subsequent updates, *available at* www.dhs.gov/privacy.

Mitigation: CBP stores information in order to provide the initial waiver adjudication and then to allow for continuous vetting of the applicant during the validity of the waiver (no more than five years). This retention is based upon operational and law enforcement needs.

CBP will retain information submitted as part of the e-SAFE website for 5 years after the ARO has rendered the final decision, which matches the 5 year maximum validity period of an approved waiver. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 17-year retention period (generally 5 years active, 12 years archived) to active law enforcement lookout records will be matched by CBP to enforcement activities, investigations, or cases, including e-SAFE applications. This retention schedule also applies to incomplete and not submitted applications, for which the retention period begins after the last account activity. As with in-person applications for waivers, CBP treats incomplete and not submitted applications as passport control inspections.

Once the information is archived, the number of officials with access to it will be further limited. Data linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including e-SAFE applications that are denied, will remain accessible for the life of the law enforcement activities to which they are related.

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.

CBP shares e-SAFE information on a case-by-case basis with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, or when DHS/CBP believes the information would assist enforcement of civil or criminal laws. Generally, ARO shares applicant information with the Department of Justice Executive Office of Immigration Review (EOIR) in the event of an appeal, and to investigatory or enforcement agencies in the event of a law enforcement or national security concern.

In addition, CBP may share e-SAFE information in bulk with federal partners for law enforcement and national security purposes, consistent with a signed memorandum of understanding (MOU).

Consistent with the A-File SORN, e-SAFE information may be shared when CBP reasonably believes such use is to assist in anti-terrorism efforts, intelligence gathering related to national or international security, or transnational crime. CBP may share information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in bulk,

to assist in counterterrorism or counter-intelligence activities, consistent with an information sharing and access agreement for ongoing, systematic sharing. CBP may also share e-SAFE information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in response to queries predicated on a specific threat to national or international security, or to assist in other intelligence activities.

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

DHS will share e-SAFE information with external organizations consistent with the published routine uses in the SORNs that cover e-SAFE, which are compatible with the original purpose of collection. Sharing with external entities for law enforcement and national security is consistent with the original purpose of collection because the information is shared when the individual's admissibility is relevant to such investigations. In the event that CBP shares e-SAFE information outside of CBP, CBP will detail the established data sharing practices in Memoranda of Understanding (MOU) and Interconnection Security Agreements (ISA), when appropriate, which govern the sharing of e-SAFE information. Under the terms of these MOUs and ISAs, other agencies will secure e-SAFE information consistent with approved security practices that meet DHS standards. Personally identifiable information will be kept secure and confidential[29] and will not be divulged to any person within or outside e-SAFE program without an official need to know. Recipients from other agencies will be required by the terms of the information sharing agreement to employ security features to safeguard the shared information.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP enters into Memoranda of Understanding/Agreement (MOU/A) with external organizations prior to the systematic sharing of information. When sharing information with parties outside of CBP, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for CBP are applied to the outside entity. Any agreements between CBP and external entities fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing.

Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, CBP includes justification for collecting the data, and an acknowledgement that the receiving agency will not share the information without CBP's permission, as applicable.

[29] e-SAFE data is stored electronically at the CBP Data Center in a compartmentalized database safeguarded by passwords, encryption of data at rest by Transparent Data Encryption, and auditing software. Data is secured in full compliance with the requirements of the DHS IT Security Program Handbook.

Information that is shared with other agencies, federal, state, local, tribal or foreign, outside of the context of any MOU or prior written agreement generally requires a written request by the requesting agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office.

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

MOUs and other written agreements defining roles and responsibilities are executed between CBP and each agency that received e-SAFE data on a systematic basis. The information may be transmitted either electronically or as printed materials to authorized personnel. Electronic communication with other, non-CBP systems, may be enabled via message/query based protocols delivered and received over secure point-to-point network connections between e-SAFE and the non-CBP system. CBP's external sharing of the data submitted to e-SAFE complies with statutory requirements for national security and law enforcement systems.

Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement generally requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data shared by CBP with external partners will be used beyond the original purpose of collection (waiver of inadmissibility determination).

Mitigation: CBP is careful to share data with external agencies that have a need to know and put the information to a use that is compatible with CBP SORNs. CBP documents these safeguards in MOUs and other written agreements with the external partners. All prospective information handlers must be authorized to access the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing the information with an external agency.

When sharing information with third parties, the same requirements related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. This criteria is determined and approved during the information sharing disclosure review process by the CBP Privacy and Diversity Office. Third parties must agree to uphold the same security and privacy measures that are used by CBP and DHS.

Section 7.0 Redress

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

Applicants may access their e-SAFE information to view and amend their application on a limited basis and view their e-SAFE status (submit application, ARO request, and determination).

Once individuals submit their personal information in e-SAFE, they will be able to access it through the e-SAFE website. Applicants can see the information they supply on the e-SAFE website as they fill out the application and again before submission, to confirm it is timely and accurate. Applicants will not be able to view any data once it has been submitted. After submission, applicants may update limited information such as change of address, e-mail, and telephone number. Applicants who do not report to the POE to complete the biometrics portion of the application will be considered to have abandoned their application after 45 days.

DHS allows U.S. citizens and Lawful Permanent Residents to seek access to information maintained in e-SAFE. Requests for access by all persons, including foreign nationals, to PII contained in e-SAFE may be submitted under the Freedom of Information Act. However, information maintained in e-SAFE pertaining to the accounting of a sharing with a law enforcement or intelligence entity is exempt from the following provisions of the Privacy Act, pursuant to 5 U.S.C. § 552a(j)(2) or (k)(2). Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, notarized and submitted under penalty of perjury.

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

Individuals have multiple options for correcting inaccurate or erroneous information:

1. Information erroneously submitted by an applicant in e-SAFE may be corrected by the applicant before he/she has paid and submitted the application. The applicant will be able to make limited updates such as (change of address, e-mail, and telephone number) after the application has been submitted. When the applicant reports to the POE for biometrics, the applicant may request that the CBP officer upload new or additional pertinent documents and/or add notes.
2. The ARO may also administratively update the data for the applicant when the applicant emails the ARO at inquiry.waiver.aro@dhs.gov. Attorneys or a properly

designated representative may ask for an update by emailing to attorneyinquiry.waiver.aro@dhs.gov and providing applicant's full name, and DOB. When the applicant presents him or herself for biometrics at the POEs, the applicant can request a correction to the application. The CBP officer will verify documentation presented by the applicant by comparing it against information entered in e-SAFE and determine whether the application may be administratively updated. Individuals whose personal information is collected and used by the e-SAFE program may, to the extent permitted by law, request correction of inaccuracies.

3. Individuals who believe e-SAFE holds inaccurate information about them, or who have questions or concerns relating to personal information in e-SAFE, can email the ARO at inquiry.waiver.aro@dhs.gov or have their designated representative e-mail the ARO at attorneyinquiry.waiver.aro@dhs.gov.

A person who believes that CBP's actions are the result of incorrect or inaccurate information may request information about his or her records pursuant to procedures provided by the Freedom of Information Act and the access provisions of the Privacy Act of 1974 by writing to:

U.S. Customs and Border Protection
Freedom of Information Act Division
90 K Street NE, 9th Floor
Washington, D.C. 20229

Travelers may also contact the DHS Traveler Redress Inquiry Program (TRIP) at 601 South 12th Street, TSA-901, Arlington, VA, 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible to identify the record(s) at issue.

Individuals who experience difficulties accessing or navigating the e-SAFE website should contact the CBP call center at 1-202-325-0180 for instructions on how to navigate the website.

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

Upon beginning an e-SAFE application, instructions and an advisory notice will be provided notifying the applicant that they are applying in e-SAFE and that the information provided can be used during inspection to determine admission. Individuals are also notified of these procedures via the website and this PIA.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk to redress for e-SAFE. CBP has well-established redress and appeal processes for applicants to seek appeal of an unfavorable determination. Individuals who have received an unfavorable determination can appeal ARO's decision by filing Form I-290B, Notice of Appeal or Motion to appeal to the following address:

U.S. Customs and Border Protection
Admissibility Review Office
Mailstop 1234
7799 Leesburg Pike, 6th Floor
Falls Church, VA 20598-1234

The applicant may also correct erroneous information through the measures listed in 7.2 of this PIA.

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?

Access to the system for internal users is limited to those personnel with a job-related requirement to access the information. All internal users with access to the system are required to have full background checks. All program managers, IT specialists, analysts, and CBP Officers, the latter assuming authorization by the e-SAFE Security Administrator, will have general access to the system. CBP contractors, in particular those involved with systems support, will also have access to the system.

Contractors to CBP may have an essential role in designing, developing, implementing, and managing the system due to their specialized expertise. Contractors must complete CBP full field background investigations before they are allowed to access any e-SAFE data and will receive the same security and privacy training as CBP Government employees.

Internal users of e-SAFE systems and records will be assigned different privileges based on their positions and roles to carry out their official duties. Audits will be conducted to log all privileged user transactions and monitor for abuse. External users, e-SAFE applicants, or their authorized agents, will only have the ability to create or update their respective "accounts" within the system.

In addition, rules of behavior are established for each major application, including e-SAFE. These rules of behavior require users to be adequately trained with regard to the security of their systems. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign

statements acknowledging that they have been trained and understand the security aspects of their systems. Rules of behavior will be posted online prior to login for internal users. In addition, the rules of behavior already in effect for each of the component systems from which e-SAFE draws will be applied to the program, adding an additional layer of security protection. Security, including access-related controls, will be certified initially and at specified intervals by the CBP Security organization through Certification and Accreditation (C&A) of the e-SAFE system.

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

All users of e-SAFE system are required to complete and pass a bi-annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and CBP policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to e-SAFE. This training is regularly updated.

DHS employees are also required to sign statements acknowledging that they have been trained and understand the security aspects of their systems and comply with the following requirements:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and e-SAFE policies and procedures.

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

The personally identifiable information collected and maintained by e-SAFE will be accessed principally by ARO employees of CBP. The e-SAFE system, using the Salesforce platform, will secure information consistent with the requirements of the DHS IT Security Program Handbook. This handbook established a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules.

In order to access e-SAFE information, a user must have a need to know, an appropriate background clearance and completed the annual privacy training. A supervisor submits the request to the Office of Information and Technology (OIT) at CBP indicating the individual has a need-

to-know for official purposes. OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Identity authentication is done via PIV cards to login to e-SAFE and UPAX.

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?

MOUs regarding the sharing of e-SAFE information will be drafted and reviewed by the program manager, component Privacy Officer, and counsel in accordance to the information provided in section 8.0 of this PIA.

Responsible Officials

Guy Cangé
Office of Field Operations
U.S. Customs and Border Protection
(571) 468-6704

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

JONATHAN R CANTOR
Digitally signed by JONATHAN R CANTOR
Date: 2019.03.12 17:31:44 -04'00'

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security