Privacy Impact Assessment
for the
electronic Travel Document (eTD) System

DHS/ICE/PIA-003

February 6, 2014

Contact Point
Thomas Homan
Executive Associate Director
Enforcement and Removals Operations
U.S. Immigration and Customs Enforcement
(202) 732-3100

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

Abstract

U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS), owns and operates the *electronic* Travel Document (eTD) System. eTD provides an efficient means for ICE personnel to request, and foreign consular officials to review and adjudicate travel document requests for aliens who have been ordered removed or granted voluntary departure from the United States but do not possess valid travel documents. The Privacy Impact Assessment (PIA) for eTD was originally published on October 13, 2006. Since that time, several technical releases have been made to improve the overall efficiency of the system, and a flag has been added to identify aliens with a criminal record, thus necessitating this update and republication of the eTD PIA.

Overview

ICE's mission is to protect America and uphold public safety. This is accomplished, in part, by facilitating the removal of aliens who are ordered removed or granted voluntary departure from the United States. eTD was created to provide efficiencies for ICE and foreign governments in filing requests and granting issuance of travel documents.

ICE Enforcement and Removal Operations (ERO) are responsible for ensuring that removable aliens in the United States are removed in a timely manner. When an alien is ordered removed from the United States, a consular official from the alien's country of citizenship must issue a travel document if required for entry into his or her country of citizenship or required by a country, which is transited in his or her removal itinerary. This travel document serves as a temporary passport that allows the alien to return to his or her country.

Not all foreign governments have elected to fully participate in the eTD process. For "non-participating countries," ICE uses eTD only to create the travel document package and the remainder of the travel document process is handled outside of the eTD system. For "participating countries," both ICE and the foreign government's consular officers use eTD for the full travel document process, i.e., to coordinate the submission, review, and update of the travel document package, as well as the certification or denial of the travel document.

The eTD system allows for correspondence to travel between ICE and foreign government officials in the travel document request process via an internet-based system. The eTD system allows foreign consular officers to electronically view travel document requests and issue travel documents from the consulate, eliminating the process of requesting travel documents by mail and ultimately contributing to more expeditious removals.

The eTD Process

In order to remove foreign nationals who have been ordered removed from the United States, ICE generally needs a valid unexpired passport or other travel document issued by an embassy or consulate to schedule and facilitate the alien's departure from the United States.

In most cases, the travel document request process begins after the issuance of a final order of removal or a grant of voluntary departure. To begin the process, ERO creates a travel document request package within eTD.

The travel document request package is a composite of documents and information used by the reviewing consular official to adjudicate ICE's request for a travel document. This information comes from four sources: the Enforcement Integrated Database (EID)[1], the DHS-owned Automated Biometric Identification System (IDENT)[2], interviews conducted by ERO officers and/or consular staff, and documents uploaded into eTD including the removal order, charging document, and additional supporting documents used by the consular official to verify the citizenship of the alien. These additional supporting documents may include copies of birth certificates, passports, marriage licenses, military discharge papers, and any other information the consular official can use to adjudicate the request for a travel document.

To create a travel document request in eTD, ERO first enters the Alien Registration Number (A-Number) in eTD to retrieve biographical information about the alien (e.g., name, immigration or naturalization status, birth details) from EID, and biometric information (e.g., left and right index fingerprints and booking photographs) from IDENT. Additional documents may be imported from EID and/or scanned and uploaded into eTD. Information from either EID or IDENT, as well as other biographical information, can be updated or modified within eTD by ERO before completing the travel document request package.

Not all foreign governments have elected to utilize the eTD system. Participating countries enter into a Memorandum of Understanding (MOU) with ICE governing their use and access to eTD, including training requirements. Under the MOU terms, consular officials for participating countries receive onsite training that addresses appropriate access to and use of eTD. Once trained, the consular officials can access the alien's biographic and biometric information in eTD, which they use to help verify the identity, nationality, and citizenship of the alien in question.

After ERO completes the travel document request package in eTD, the process differs for participating and non-participating countries.

For non-participating countries, the package is tracked by the shipping carrier to confirm delivery, and ERO follows up with the consulate if a response is not received within a reasonable time. Once the consular official has adjudicated ICE's request for a travel document, the official will either issue or deny the travel document, and ship the travel document or denial decision back to ERO using the provided self-return envelope. ERO then scans the travel document or denial decision into eTD, updates eTD with the outcomes, and enters the issued and expiration dates for any travel document issued into the relevant eTD data fields.

---

[1] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) PIA, January 14, 2010, and multiple updates at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf.
[2] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA, December 7, 2012, at http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_usvisit_ident_appendixj_jan2013.pdf.

For participating countries, consular officials access eTD directly using their own unique user ID and password to view information, upload documents, modify personal details of the alien in the appropriate data fields, verify the citizenship of the alien, and issue travel documents. In some cases, the consular official may elect to interview the alien. If the consular official is satisfied that the alien is a citizen of his or her country, the travel document is electronically issued and signed in eTD[3] by the consular official. If the consular official does not agree to issue a travel document for the alien, he or she indicates the denial in eTD, as well as the reason for denial. Once the travel document has been issued, the ERO and consulate users no longer have the ability to update fields for that record within eTD. The ERO employee prints the travel document from eTD.

Each time an ERO user submits travel document requests to a consulate within eTD, the system sends transactional information to EID. This information includes the alien's A-Number, first and last name, date the request was submitted to the consulate, and the status of the request. eTD updates the status information in EID when a request status changes from pending to issued or denied. Similarly, if an alias name is provided by the consulate users, eTD will update EID with the alias first and last name. EID does not retain a copy of the issued travel document submitted within the eTD system.

Once the travel document is issued, ERO makes travel arrangements for the alien's departure from the United States, and places a paper copy of the travel document in the alien's A-File, along with any new supporting documentation not already in the alien's A-File.

eTD Today

Since the initial implementation of eTD in 2006, ICE has made several upgrades and/or technical enhancements to eTD, including: creating a link in EID with single sign-on capability to eTD for ERO employees with access to eTD, providing better data search capability, automatically populating additional data fields from EID during the creation of the travel document package (e.g., detention location and final order date), producing cover letters for non-participating countries and case summaries for participating countries that list supporting documents in the travel document request, expanding report capability, and building in checks and balances using the A-Number to avoid duplicative travel documents or unnecessary travel documents for aliens who are reported deceased or whose case was closed.

In addition to these technical enhancements, eTD now searches EID to determine if the alien has any criminal convictions. This information is used to create a criminal indicator flag, i.e., criminal or non-criminal within eTD. The flag is used for sorting and statistical purposes and does not identify the specific crime for which the alien has been convicted within the data fields. However, given that eTD allows ERO employees to upload scanned documents into eTD, criminal information may be included in these uploaded documents.

[3] In some cases, the consular officials elect to sign the travel document and provide a hard copy to ICE.

Lastly, ERO staff is working with the ICE Privacy and Records Office to develop a records schedule. Upon approval of the pending record schedule, the following retention schedule will be implemented.

Seven days after a decision has been made concerning the travel document request, the issued or denied travel document and the A-Number, first name, last name, and middle name will be archived. The archive will reside in attached storage within the DHS-owned data center and will be retained for twenty years. The proposed twenty-year retention schedule increases the ten-year retention schedule proposed in the original PIA. The twenty-year retention schedule for the travel document runs concurrent with the maximum ban (exclusive of the lifetime ban) imposed on aliens who have been banned from re-entering the United States. Possession of a travel document, previously issued by the alien's country of citizenship, facilitates the removal of the alien. A printed copy of the travel document, along with any new supporting documentation not already in the alien's A-File, will be placed in the alien's A-File and becomes subject to the current A-File retention schedule.

Within the same seven-day period, the remaining biographic and biometric information within eTD including fingerprints, pictures, supporting identification documentation (e.g., passport, birth certificate, national identification cards), and home address will be deleted or destroyed.

The user information obtained to grant access to consular officials will be retained until the eTD System Administrator is notified by the foreign consulate to remove the user from the system. The ERO employee information will be retained until the end of the sixth fiscal year after the ERO employee separates from ICE.

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?

ICE is authorized to collect this information pursuant to 8 U.S.C. § 1231(a) and (b). The statute authorizes ICE to collect and maintain information relevant to the removal of unlawful aliens, including obtaining travel documents from foreign countries to which they will be removed.

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

The DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) SORN (May 3, 2010, 75 FR 23274), and the DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORN (November 12, 2012, 77 FR 70792) apply to the information maintained in eTD.

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

eTD renewed the Authority to Operate (ATO) on August 20, 2011. This ATO is valid for three years, expiring August 19, 2014.

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

No, ERO is working with ICE Privacy and Records staff to develop a records schedule for review by NARA. It will propose the retention periods for eTD records as described in Section 5.

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.

To gain access to eTD, each foreign consular official is required to complete the Electronic Travel Document System Access Request Form – Consular Official/Foreign National; therefore, the system is subject to the requirements of the PRA. ICE is currently working to obtain authorization for this collection of information under the PRA from the Office of Management and Budget (OMB).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

eTD collects, uses, maintains, or disseminates information on three categories of individuals: (1) aliens who have been ordered removed or who have been granted voluntarily departure from the United States; (2) family members of these aliens; and (3) eTD users, namely consular officials and ERO employees. The type of personally identifiable information collected and maintained within eTD varies with the individual's category.

Alien Information

Biographic information includes: name; alias(es); address(es); nationality; citizenship; date of birth (DOB); place of birth; physical description; detention location; status of removal request; identification numbers such as A-Number, passport number, driver's license number, and social security numbers (SSN); documents such as birth and baptismal certificates, marriage licenses, Military Records, national identification cards; and any other information useful in identifying the alien as a citizen of the consular official's country.

Biometric information includes photographs and fingerprints.

Criminal information includes a criminal flag identifying whether the alien has been convicted of a crime. In addition, uploaded documents also may contain data about the alien's criminal and arrest history.

Alien Family Member Information

Information about the alien's parents, spouse, partners, children, and other relatives may include: name, relationship to alien, address(es), DOB, place of birth, nationality, citizenship, date and place of marriage to alien, and ages of children.

Consular Official and ERO Employee Information

Information about consular officials and ERO Employees includes: name, title, work address, work phone numbers, and email address. In addition, the consular official provides citizenship information, DOB, city of birth, and country of birth. The ERO employee provides field office and sub-office if applicable, and the employee's Password Issuance and Control System (PICS)[4] user ID, which is needed to access eTD. An ERO employee must have an active PICS user account and password to be granted access to eTD.

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

eTD obtains information from four main sources, namely: EID, IDENT, documents provided by the alien being removed, or interviews with the alien being removed. eTD also obtains information from foreign consular officials and ICE employees, as necessary for access approval. Specific information for each category of individuals originates from the following sources:

Alien Information

When the ERO employee enters the alien's A-Number into eTD, alien information is automatically populated into eTD through EID and IDENT. Supplemental information may also be collected from the alien during interviews with ERO or consulate users and entered directly into existing eTD fields. Additional supporting documents may be collected from the alien and uploaded into eTD by ERO employees, including birth or baptismal certificates, passports, marriage licenses, military discharge papers, and any other documents that help to verify the alien's citizenship. The removal order, charging document, and Information for Travel Document or Passport, also known as DHS Form I-217, may provide additional information about the alien, including criminal history, if applicable. These documents are provided directly from EID or manually uploaded by an ERO employee. Biometric information is obtained directly from IDENT but can be updated by the ERO employee. Additional information may be obtained during ad hoc interviews between the alien and ERO employees or consular officials.

Alien Family Member Information

Information about the alien's family members may be obtained directly from EID, DHS Form I-217, interviews with the alien being deported, and documents provided by the alien such as birth or baptismal certificates and marriage licenses. The information on DHS Form I-217 is collected when the alien is apprehended or detained using the information provided by the alien, available identity or travel

[4] *See* DHS/ICE/PIA-013 Password Issuance and Control System (PICS) PIA, November 24, 2009, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_pics.pdf.

documentation, and other available biographic information. This form may be obtained directly from EID or uploaded by an ERO employee.

Consular Official and ERO Employee Information

Information is collected directly from the consular official using the Electronic Travel Document System Access Request Form – Consular Official/Foreign National and from the ERO employee using the Electronic Travel Document System Access Request Form – ERO. When the individual completes the form and it is approved by the supervisor or consulate official, it is submitted to the System Administrator[5] for access approval.

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

eTD does not use information from public or commercial sources.

2.4 Discuss how accuracy of the data is ensured.

Some information stored in eTD is provided by the person who is the subject of the record. This information may include documents such as birth certificates, passports, and other identity documents. Additionally, information from EID and IDENT is merged, reviewed, and compared with the respective alien's documentation by an ERO employee for accuracy prior to being sent to a foreign consular official. Records are matched using either an A-Number or an event identification number, which is a number used by EID to identify a particular encounter. If there is a question regarding the merging of the information, it may be verified through an interview with the respective alien.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: It is possible that, accidentally or purposefully, erroneous or biased information may be uploaded to eTD.

Mitigation: During the initial encounter, information is collected directly from the alien and entered into EID. In addition, the merged information from different systems is reviewed in eTD by an ERO employee and the foreign consular official. If the merging of the data exposes inconsistencies in the information maintained regarding the alien, or if other questions of fact arise, ERO can further verify the accuracy of the data by interviewing the alien.

[5] The System Administrator performs a different role than the System Owner. The System Administrator provides technical support and assigns user roles. Whereas, the System Owner is responsible for the overall eTD application and maintains a list of third-party disclosures.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The ERO employee uses the information in eTD to create a travel document package for review by the consular official to verify the identity and citizenship of the alien ordered removed from the United States. The consular official uses the information to determine if the alien is a citizen of the official's country. If the travel document package provides sufficient information to identify the alien as a citizen of the official's country, the official can issue a travel document and the alien can be removed. The consular officials may use the criminal information to determine if additional procedures will be required when receiving their returning nationals, such as requiring face-to-face interviews.

Alien Information

eTD collects biographic and biometric information, including fingerprints, relating to aliens who have been ordered removed from the United States, or who are voluntarily departing the United States but do not have valid travel documents. This information is used by the ERO employee to verify the identity of the alien and create a travel document package, which is then submitted to the foreign consular officials. Consular officials use the information so they may verify the citizenship of the individual and issue the travel documents required for ICE to remove the individual to their country of citizenship. In addition to the biographic information provided by the documents and database, the fingerprints provide another way for consular officials to verify the alien's identity, and the criminal information serves as an alert should additional procedures be required when receiving returning nationals.

Alien Family Member Information

eTD collects family member information to provide another way to verify the alien's identity and citizenship. Family information such as names, addresses, dates and places of birth, nationalities, and family relationships is used by the ERO employee to provide additional documentation in the travel document package to identify the alien as a citizen of the consular official's country. Consular officials may use the familial information in the travel document package as an additional way to verify the alien's citizenship using their own record systems. Once verified, consular officials are able to issue a travel document.

Consular Official and ERO Employee Information

eTD collects consular official and ERO employee information directly from the individual using an access request form provided by the System Administrator and approved by an ERO supervisor or consular official. The information is collected to control access to eTD and prevent unauthorized use. Access to eTD allows ERO employees to create the travel document package and consular officials to review, approve, or deny the request, and issue the travel document.

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, eTD does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

No other DHS components have access to eTD.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that eTD users will use the system for purposes beyond what is described in this PIA.

Mitigation: Proper use of eTD is controlled in several ways. eTD incorporates user roles that limit user capabilities. They are assigned by system administrators, and based upon the user's job function and need-to-know. At least annually, reviews of system users are performed to re-certify users and identify any unauthorized access. DHS information security policies for sensitive systems are in place to provide clear instruction on the proper use of the system. Technologies are in place to enforce those policies through the use of user names, user roles, session inactivity timeouts, restricted data fields, an approved banner reminding the user of the proper use of the system, and user passwords. Passwords must meet complexity requirements, and expire every 30 days, thus requiring the user to change the password. User accounts that remain inactive after 45 days are disabled.

Audit logs are reviewed by the Information System Security Officer (ISSO) on a quarterly basis to detect any unusual activity within eTD. In the event that unusual activity is identified, the ISSO conducts further investigation of the activity. Disciplinary action for violations of ICE policies regarding the system is taken when warranted. Before receiving access to the system, all users are trained on system use and other policies governing the system such as privacy and security policies.

With the exception of the issued travel document, the A-Number, and alien's name, all information retained within eTD for a travel document request including all biographic and biometric information within eTD data fields, and uploaded documents will be deleted from eTD seven days after the consular official has made a decision concerning the travel document request. A printed copy of the issued travel document, along with any new supporting documentation not already in the alien's A-File, will be placed in the alien's A-file and will become subject to the current A-file retention schedule.[6]

[6] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN (June 13, 2011, 76 FR 34233) at http://www.gpo.gov/fdsys/pkg/FR-2011-06-13/html/2011-14489.htm.

Consular officials seeking an archived copy of the travel document will submit a request to the ERO employees assigned to their consulate office.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Prior notice is provided by the DHS/ICE-011 ENFORCE SORN, which covers the collection of information about or from individuals who fail to leave the United States after receiving a final order of removal or who fail to report to ICE for removal after receiving notice to do so. Prior notice is also provided by the DHS/ALL-004 GITAARS SORN, which covers the collection of information from ERO employees to control access to eTD and prevent unauthorized use.

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

At the time of arrest and/or detention by ICE, the alien is asked to provide biographical information relating to his or her citizenship and/or nationality. When detained by ICE, this information is entered into EID and made available to eTD. Therefore, the alien does not have the opportunity to consent to the uses of his or her information, decline to provide the information, or opt out of providing the information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a potential risk that the general public is not aware of the existence of eTD and that information pertaining to a specific individual exists in eTD.

Mitigation: The publication of the eTD PIA and the subsequent PIA updates mitigate this risk by providing a detailed description of the types of individuals whose information is contained in the system, the types of data it contains, and how the data is used.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

ERO staff is working with the ICE Privacy and Records Office to develop a records schedule. Upon approval of the pending record schedule, the following retention schedule will be implemented:

Seven days after a decision has been made concerning the travel document request, the issued or denied travel document and the A-Number, first name, last name, and middle name will be archived. The archive will reside in attached storage within the DHS-owned data center and will be retained for twenty years. The proposed twenty-year retention schedule increases the ten-year retention schedule proposed in the original PIA. The twenty-year retention schedule for the travel document runs concurrent with the maximum ban (exclusive of the lifetime ban) imposed on aliens who have been banned from re-entering the United States. Possession of a travel document, previously issued by the alien's country of citizenship, facilitates the removal of the alien. A printed copy of the travel document, along with any new supporting documentation not already in the alien's A-File, will be placed in the alien's A-File and becomes subject to the current A-File retention schedule.

Within the same seven-day period, the remaining biographic and biometric information within eTD including fingerprints, pictures, supporting identification documentation (e.g., passport, birth certificate, national identification cards), and home address will be deleted or destroyed.

The user information obtained to grant access to consular officials will be retained until the eTD System Administrator is notified by the foreign consulate to remove the user from the system. The ERO employee information will be retained until the end of the sixth fiscal year after the ERO employee separates from ICE.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in eTD will be retained for longer than necessary and appropriate given the purpose of the system and the original reason the information was collected.

Mitigation: Information is retained in eTD only as long as necessary and appropriate to facilitate the issuance of a travel document. Seven days after a decision has been made concerning the travel document request, a limited set of information consisting of the issued or denied travel document and the following eTD data fields are archived: A-Number, first name, last name, and middle name. The archive will reside in attached storage within the DHS-owned data center and will be retained for twenty years. In addition, a printed copy of the travel document will be placed in the alien's A-File and becomes subject to the current A-File retention schedule.

Within the same seven-day period, the remaining biographic and biometric information including fingerprints, pictures, supporting identification documentation (e.g., passport, birth certificate, national identification cards), and home address will be deleted or destroyed. Thus, only a limited set of information is retained longer than seven days to maintain a record of the travel document issued and the identifying information needed to link the travel document with the appropriate alien.

Consular official user information will be maintained for user accessibility for as long as the user needs access to eTD to perform his or her duties as determined by the consulate. ERO employee

information will be retained until the end of the sixth fiscal year after the ERO employee separates from ICE.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Yes, information maintained in eTD is shared with the consular officials of foreign countries. The information shared with the consular officials is restricted to those aliens whom ICE is seeking to return to that official's country pursuant to a removal order or grant of voluntary departure. The information within eTD is used by consular officials to determine the citizenship and/or nationality for a selected alien for the purpose of issuing a travel document needed to remove that alien from the United States. Once the alien's citizenship and/or nationality has been verified, the consular official can issue a travel document to effect the alien's repatriation. The foreign consular official may maintain electronic or paper copies of the relevant information.

Non-participating countries are provided with the information in hard copy by mail, whereas participating countries access the information directly via eTD. Foreign consular officials of participating countries access information in eTD through their eTD user account via the Internet using a Secure Socket Layer web portal technology. Each official's access to eTD is subject to ICE's approval.

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

The sharing of PII with consular officials outside of the Department is compatible with removal purposes of the original collections listed in the SORN. The SORN includes information about the removal of individuals who fail to leave the United States after receiving a removal document. The SORN supports the sharing of PII with foreign governments for the purpose of coordinating and conducting the removal of aliens to other nations.

6.3 Does the project place limitations on re-dissemination?

Yes, the MOU signed by participating countries to gain direct access to eTD specifies that the foreign government may not further disclose information to third parties without written permission from ICE. MOUs entered into with participating countries set forth ICE's security and information handling requirements. The MOUs contain provisions for the termination of the MOU in the event a participating government fails to comport with the expectations contained in the MOU. The foreign government users are aware of these disclosure restrictions because all users are provided with System Security training

regarding access and disclosure of information. ICE also maintains audit logs of the foreign government users of the system.

When participating countries request permission to disclose information from eTD to a third party and ICE has approved such disclosures, the ICE System Owner manually tracks these disclosures in a log. The log contains the date the request was made, document requestor name and organization, participating country, determination of the request, and how the information was delivered.

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

Records of disclosures made by ICE outside of DHS are maintained primarily in audit logs within eTD. The audit logs allow ICE to track information shared with participating countries by identifying actions performed by individual users in the system. In addition to identifying the individual user, the logs identify when requests for travel documents were created, submitted, reviewed, and issued. eTD access is limited to consular officials of participating countries who have been approved by the consular general, the top official in the consulate, and verified by the System Administrator with the embassy.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data within eTD will be shared with external parties lacking a need-to-know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: Several controls are in place to limit information sharing from eTD to those with a need-to-know and to properly record external sharing. First, foreign consular officials using eTD are assigned user roles to limit the data to which they have access. As a result, they can only access information about those aliens requiring travel documents to return to the home country of the consulate. Second, eTD uses internal audit logs to track information shared with consular users. These logs identify individual users, when these users accessed the system, and what actions these users performed while in the system. Third, third-party information sharing is controlled by the provisions of the MOU. According to the MOU, the foreign government may not disclose information to third parties without written permission from ICE. Finally, the MOU also contains provisions for the termination of activities under the MOU in the event a participating government fails to comport with the expectations contained in the MOU.

Privacy Risk: There is a risk that the travel document package will become lost when sent via hard-copy to the consulate of a non-participating country.

Mitigation: ERO sends hard copies of the travel document package to consulates of non-participating countries using a national shipping carrier with the ability to track the package and confirm delivery. ERO uses the carrier provided envelopes and requires a delivery receipt signed by a consulate staff member when the package is received. During the delivery process, the carrier provides a real-time, online tracking system for use by ERO to determine the location of the package at any point in the process. If the package is not delivered in a reasonable time, ERO can alert the carrier, who can conduct a physical search using the recorded tracking history to determine the present location of the package. In

addition, ERO follows up with the consulate if a response to the travel document request is not received within a reasonable time.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking notification of and access to any record contained in eTD, or seeking to contest its content, may submit a request in writing to the ICE FOIA Officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests.

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

Prior to removal, the individual is given the opportunity to identify any erroneous information in his record during meetings with U.S. government officials and/or foreign consular officials. If errors are identified, authorized eTD users are able to edit/correct the erroneous information in eTD, or in other systems from which the data is pulled into eTD (EID or IDENT). Once the individual has been removed, inaccurate or erroneous information can be corrected using the correction procedures described in Question 7.1 above.

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

Upon entry into a detention facility, detainees receive a copy of the detainee handbook. The purpose of the handbook is to provide detainees with an overview of detainee rights and responsibilities while residing at the facility. In addition to the right to legal representation, detainees are informed that they may ask an ICE officer or facility staff for copies of documents in their A-File, detention files, or medical record. If errors are identified, authorized eTD users are able to edit/correct the erroneous information in eTD, or in other systems from which the data is pulled into eTD (EID or IDENT).

Instructions about how individuals may correct their information is made available through the publication of this PIA and the DHS/ICE-011 ENFORCE SORN (May 3, 2010, 75 FR 23274).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Given that the individual is being removed from the United States, there is a risk that individuals will have limited opportunity to access and redress their data as maintained in this system.

Mitigation: Individuals provide their information at the time of their initial encounter. Subsequent interviews may or may not require the alien to verify information. ERO relies on the biographical information provided by the individual and entered into ENFORCE. This information may be provided by sworn statement or by surrendering identity documents.

Specific access and redress provisions are covered in the Notification Procedure section of the DHS/ICE-011 ENFORCE SORN. In most cases, redress for information that is incorrect is usually handled prior to removal. Should an alien indicate that information the U.S. Government has about him or her is inaccurate, he or she has the opportunity to provide correct information either at arrest or during a meeting with a consular official in order to generate a travel document. In addition, the alien may notify an ICE officer during regular staff-detainee communications and/or call the toll-free Community and Detainee Helpline to report unresolved issues, including redress of inaccurate information. Additionally, with or without the assistance of a lawyer, the alien may submit a FOIA request to find out whether the information is accurate.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

eTD uses various technological and policy-based controls described below to help ensure that eTD information is used in accordance with the stated practices in this PIA.

Access Controls: eTD has System Administrators who assign user roles based upon the user's job responsibilities and need-to-know. Foreign consular officials using eTD are assigned user roles to limit the data to which they need to have access, that is, they can only access information about those aliens requiring travel documents to return to the home country of the consulate. ERO employees are assigned user roles based upon an individual's job needs and approval from the user's supervisor and System Owner.

User and System Audits: Through the use of audit logs, the ISSO monitors activity to ensure that the information within eTD is used as stated in this PIA. Audit logs for eTD capture the specific action taken, the user who performed the action, and the date and time the action was performed. Examples of actions recorded in the log include creating, submitting, viewing, and issuing a travel document in response to the request. Access to these logs is restricted to the eTD system and security personnel such

as the ISSO. The ISSO reviews the logs to identify unusual activity and/or improper use on a quarterly basis. Unusual activity or improper use, such as unusual patterns or trends, are further investigated. Disciplinary action for violations of ICE policies regarding the system is taken where warranted. Before receiving access to the system, all users are trained by ICE staff on system use and other policies governing the system such as privacy and security policies.

MOUs with Participating Countries: The MOU requires consulate users from foreign countries participating in the eTD program to immediately report to ICE any suspected improper access or use of the system. Failure to make such reports may result in the termination of the MOU and termination of access to eTD. Again, consular officials are assigned user roles to limit the data to which they have access, i.e., they can only access information about those aliens requiring travel documents to return to the home country of the consulate.

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

All personnel who have access to eTD, including foreign consular officials, are required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior. No additional privacy training is provided as part of the eTD. eTD is only a new mechanism for processing hardcopy travel document requests. Training requirements remain standard for those users accessing a DHS-owned system such as eTD.

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

As stated in Section 8.1, eTD system administrators assign user roles that limit user capabilities given the user's need to know and responsibilities in the travel document process. Each user given access to eTD is required to complete an access request form that is signed by the user's supervisor. Access request forms are forwarded to requestors by the eTD system administrator. For ERO employees, the forms signed by their ERO supervisors are returned to the System Owner, who approves and maintains them. For consular officials, the forms are approved and signed by the Consul General, who is the top official at the consulate. The consular official returns the signed form to the System Administrator, who verifies the consular official's authority to access eTD with the country's Embassy. Once the access request is verified by the Embassy, the System Administrator creates the account and forwards the form to the ERO System Owner, who will maintain it. DHS ICE performs annual user reviews of eTD to ensure security and role integrity. The following are eTD's user roles:

ERO User: The ERO user is an ERO employee who is granted permission to access eTD on the intranet using either the eTD URL or from EID using the single sign-on link. All ERO users have the ability to enter/upload the data and records required to create travel document requests and document the results of the travel document request, issued or denied. In addition, ERO users can print the travel document requests from eTD and ship the package to consulates of nonparticipating countries for review and approval.

Consular Official: The consular official is a user from a participating country who is granted permission to access eTD via the Internet. Consular Officials' access is restricted to information for those aliens whom ICE is seeking to return to that official's country pursuant to the removal order. These users can view the uploaded data and records, update selected personal data fields for the alien, and issue, hold, or deny the travel document

System Administrator: The System Administrator role is comprised of members of the eTD technical support team. These users administer the system, and grant privileges to create accounts. They can add and edit users, field offices, consulates, system notifications, and travel document requests. Upon appeal by an ERO employee, they also can rescind travel document requests. System Administrators may revoke a user's access when no longer needed or permitted.

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?

All MOUs are reviewed by the program manager, System Owner, ISSO, Office of International Affairs, and the foreign government pursuing participation within eTD. Once in final draft, the ICE Privacy Office and the Office of the Principal Legal Advisor also review MOUs for privacy and legal compliance.

Responsible Officials

Lyn Rahilly, Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security