Privacy Impact Assessment
for the

Electronic Travel Document System

(*e*TD)

October 13, 2006

Contact Point
Robert B. Shiflett
Office of Detention and Removal Operations
Immigration and Customs Enforcement
(202) 732-2931

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The *Electronic* Travel Document System (eTD) will maintain personal information regarding aliens who have been ordered removed or have been removed from the United States. The eTD will also maintain information on U.S. government employees and foreign consular officials required to access the system. The eTD system will present and share alien information with the foreign consular officials and associated governments for their use in the expedited issuance of travel documents.

Introduction

The *Electronic* Travel Document System (eTD) is owned and operated by and for the United States Immigration and Customs Enforcement. The removal of aliens ordered deported, excluded, inadmissible, or removed from the United States is one of the missions of the Department of Homeland Security, Immigration and Customs Enforcement.

When an alien, other than a Mexican national, is ordered removed from the Unites States, a consular official from the alien's country of origin must issue a travel document. This travel document allows the alien to return into his or her country. Currently, there are two methods for issuing travel documents. Under the first method, the alien is transported to a foreign consulate, a consular officer interviews the alien and makes a determination of citizenship, and then the consular officer issues a travel document. As a detention facility may be several hundred miles away from a foreign consulate, the logistics involved in transporting aliens to a foreign consulate can be daunting. The second method of issuing travel documents requires the consular officer to travel to the detention facility, interview the alien and make a determination of citizenship, and then issue a travel document. The drawback here is that aliens remain in detention for days, if not weeks, awaiting an interview with a consular officer. With this method, a tremendous amount of money is expended in detention costs.

The objective of the eTD is to more efficiently present information to a deportee's respective consulate to make a determination and/or verification of citizenship and/or nationality. Once the alien's citizenship and/or nationality has been verified, the consular official can issue a travel document to affect the alien's repatriation. These travel documents are necessary to affect the order of removal of aliens from the United States.

The eTD application will allow foreign consular officials to electronically certify travel documents from a remote location, such as the Consulate, thus in many cases removing the requirement for a consular officer to visit the detainee in person. Once certified, the travel document can be printed at the consulate or from any field office. This means that an interview may not be necessary prior to generating the travel document.

To begin the process, the ICE removal team processor will query the ICE databases, Enforcement Integrated Database (EID) and IDENT, the DHS system with biometric information, to gather the individual's removal documents, data, and biometric information. This information is reviewed to verify that the correct record has been accessed. The removal order and other relevant documents are scanned

into the eTD system. This electronic package of information is then submitted and available for the foreign consular officials to view and continue processing.

The consulate is notified that an electronic travel document package is ready for review. The consular official accesses the eTD system using his unique user ID and password. The electronic documents and data are reviewed and if the consular official is satisfied that the individual is a national of their country, the travel document will be electronically certified and signed without requiring an in-person interview.

Once the electronic travel document is certified, the removal team processor will print the actual travel document at the removal office. The eTD system will streamline the removal process and reduce transportation and detention costs.

Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested and the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

The information to be collected by this system will be limited biographic and biometric information relating to aliens who have been ordered deported, excluded, inadmissible, or removable from the United States. The respective alien provided the information from the EID at the time of encounter. Additionally, limited biographical information (name and work address) will be gathered to create user profiles for ICE and foreign consular officials.

For identification purposes, eTD collects and/or disseminates biographic and biometric information for removable aliens, which includes first name, last name, fingerprints, picture, supporting identification documentation (i.e. passport, birth certificate, national identification cards), and home address.

1.2 From whom is information collected?

Information is collected from the alien being deported, foreign consular officials, and ICE employees, as necessary. Alien information is populated through the EID, a central repository for DHS enforcement data, and IDENT, which stores biometric and limited biographic data collected for national security, law enforcement, immigration, intelligence, and other mission-related functions. Additional information may be gathered from the alien during an interview.

1.3 Why is the information being collected?

The information is being collected for presentation to an alien's respective foreign consular official for the expressed purpose of expediting the issuance of a travel document to affect his or her removal pursuant to an order of removal.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

8 U.S.C. 1231(a) and (b). This is ICE's legal authority for taking removal actions, which includes obtaining travel documents from foreign countries to which ICE removes the aliens.

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

The scope of the information collected is limited to the information necessary to appropriately determine the citizenship and/or nationality of the alien as part of the removal process, and properly generate a travel document for the alien. To the extent possible, the information is collected from the alien. This could occur at the initiation of the removal and/or at the time foreign consular official finalizes the travel documents.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The eTD will be used to provide biographic and biometric information to foreign consular officials of a country to which the selected alien is being referred for the issuance of a travel document that will affect that alien's removal from the United States. The foreign consular officials will use this information to verify the identity, nationality, and citizenship of the alien so that they may issue travel documents allowing the removal of the alien to their country.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

No. Audit trails are examined to verify appropriate user conduct. Auditing information is covered at length in Section 8.0.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Some information stored on the eTD system is provided by the person who is the subject of the record. In addition, information from EID and IDENT will be merged, reviewed, and compared with the respective alien's documentation by an ICE official for accuracy prior to being sent to a foreign consular officer. Records are matched using either an Alien Number or an event

identification. This documentation includes but is not limited to birth certificates, passports, cedulas, and other identity documents. If there is a question regarding the merging of the information, it may be verified through an interview with the respective alien.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The eTD system will incorporate user roles to limit user capabilities. An administrator will assign roles as necessary for each user. Quarterly audits of the system are performed to identify any unauthorized access. Additionally, the merged information from different systems is reviewed by an ICE agent 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, ICE can further verify the accuracy of the data by interviewing the detainee.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

Information that is imported from the EID and IDENT databases will be maintained in the live eTD system for no more than 180 days. Documents relating to the issuance of the travel document will be archived as a document file in Adobe Acrobat Portable Document File format (Travel Document PDF) after no more than 90 days. Once archived, the Travel Document PDF will be maintained as part of the alien's electronic A-file and will be subject to the retention schedule for the A-file System of Records.

The information will also be archived in Adobe Acrobat Portable Document File format in the eTD system. Only the system administrator has access to the information so archived in eTD. The system administrator would only access this information if specifically requested by an ICE officer to determine whether a particular alien had previously been issued travel documents through the eTD system. This information would be helpful in verifying an alien's nationality in order to affect removal. The eTD user information will be maintained until the administrator is notified to remove the user from the eTD system. ICE proposes that the audit information for the eTD system be maintained in the eTD system for ten years.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Approval by NARA of the retention schedule is pending.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information maintained for 180 days is maintained for removal processing and only during the removal timeframe. Archived Adobe Acrobat Portable Document File format files will be used for future reference on an as needed basis for purposes described in Section 3.1. U.S. government and consular user role information is maintained for user accessibility for as long as the user needs access to eTD to perform his or her duties.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

Within the agency, only the ICE Office of Detention and Removal Operations will have access to the eTD system. Additional information gathered for the purpose of obtaining travel documents and entered into the eTD system is not shared with any other systems.

4.2 For each organization, what information is shared and for what purpose?

Not applicable. No other offices within ICE or other DHS components will be accessing the eTD system.

4.3 How is the information transmitted or disclosed?

Not applicable. No other offices within ICE or other DHS components will be accessing the eTD system.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Not applicable. No other offices within ICE or other DHS components will be accessing the eTD system.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

Officials from the consulates of foreign countries will have access to information stored in the eTD system with respect to aliens whom ICE is attempting to return to such foreign countries pursuant to orders of removal issued by ICE or the Executive Office of Immigration Review. Such foreign officials' access to the eTD system is subject to ICE's approval. This information is provided to the consular officers for their use in the issuance travel documents affecting the orders of removal. The foreign consular officer will access this information via the internet through a Secure Socket Layer web portal.

5.2 What information is shared and for what purpose?

The eTD system will be utilized to provide biographic and biometric information relevant to determining citizenship and/or nationality for a selected alien for the purpose of issuing a travel document. 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. These travel documents are necessary to carry out the order of removal of aliens from the United States. The foreign consular official may maintain electronic or paper copies of the relevant information.

5.3 How is the information transmitted or disclosed?

All information presented will be accessed through the eGovernment secure internet environment. Authorized foreign consular officers will access this information via the internet through a Secure Socket Layer web portal. ICE will use reasonable physical, electronic, and procedural safeguards to appropriately protect the information maintained in eTD against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification or deletion. Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including the encryption of all personal identifying information and all other FOUO information held on portable media such as data tapes, CDs, or laptops.

Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including the encryption of all personal identifying information and all other FOUO information held on portable media such as data tapes, CDs, or laptops.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

A Memorandum of Understanding (MOU) will be completed for each participating government. The MOU will specify system security through encryption and other system safeguards and will detail expected behaviors of the parties with regard to safeguarding information. Failure to abide by the terms of the MOU will result in the immediate termination of activities under the MOU.

5.5 How is the shared information secured by the recipient?

The information is maintained on the eTD system. There are no recipients other than the governments participating in the eTD process. MOUs entered into with participating governments will set forth ICE's expectations for security of the information. The MOU will contain provisions for the termination of the MOU in the event a participating government fails to comport with the expectations contained in the MOU.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Outside users will receive user training prior to receiving access to the eTD system. The consular user will receive four hours of formal training. This training will cover appropriate access and use of the eTD system. See the attached ISA for additional information. ICE will provide technical representatives to train designated personnel on the appropriate methods to access and retrieve information from the eTD through the ICE eGovernment website.

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

Information that is provided to external users through the eTD system relates to aliens to whom an order of removal has been issued. According to the MOU, foreign government may not disclose information to third parties without written permission from ICE. 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.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

This is not a "System of Records" within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(2), (3), and (5) since persons whose information is maintained in the system are subject to orders of removal and therefore are neither lawful permanent residents nor United States citizens. Accordingly, the agency has not published a system of records notice for the eTD system. To the extent information contained in the system was collected from the alien on various immigration forms used by DHS, such forms generally contain privacy notices indicating that the information being submitted on the form may be disclosed for law enforcement purposes.

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

The alien is required to provide biographical information relating to his or her citizenship and/or nationality.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Notice issues are not present in the eTD system. The alien being deported is already on notice regarding their deportation and the fact that the U.S. government has collected information about him/her. The eTD system allows for easy verification of that information (specifically citizenship), and permits consular access for easy generation of travel documents. No new information is being collected unless information is found to be inaccurate.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

The individual can request access to information utilizing established procedures through the Freedom of Information Act at the following address:

FOIA/PA Section
Information Disclosure Unit
Mission Support Division
Office of Investigations
U.S. Immigrations and Customs Enforcement
425 I Street, NW - Room 4038
Washington, D.C. 20536
Phone: (202) 353-8906 Facsimile (202) 616-7612

7.2 What are the procedures for correcting erroneous information?

An individual has an opportunity to correct information while meeting with U.S. government officials and/or foreign consular officials prior to deportation. Any erroneous information and subsequent data corrections are entered by U.S. government employees and/or foreign consular officials who have authorized access to the eTD system.

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

Individuals are given the opportunity to verify their information at the time of their initial encounter. Subsequent interviews may not require the deportee to verify information, provided that a prior travel document had been issued previously. A consular official may issue a travel document without meeting with the deportee.

7.4 If no redress is provided, are alternatives are available?

Immediate redress is provided in that the deportee has at least one, if not two chances to correct information.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

This system is not covered by a System of Records Notice under the Privacy Act of 1974, as amended. As such, specific access and redress provisions are not central to the functioning of the system. Should a deportee indicate that information the U.S. government has about them is inaccurate, they have the opportunity to provide correct information either at arrest, or during a meeting with a consular official in order to generate a travel document. Additionally, the deportee may submit a FOIA request to find out whether the information is accurate.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

User groups will include employees within the ICE Office of Detention and Removal Operations who have a need to access information contained in eTD in connection with their responsibilities for obtaining travel documents for aliens who have been ordered removed from the United States. In addition, the user groups will include foreign consular officials who have been authorized by ICE to access eTD in connection with their official responsibilities to provide travel documents to the Unites States with respect to aliens ordered removed to their respective countries. ICE systems administrators and ICE security officials will also have access in order to carry out their official duties relating to system maintenance and system security.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. The contractors will be responsible for system administration, maintenance, and future enhancements. The contractors will not be using the eTD system in a production capacity.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Roles are based on the necessary user groups outlined in Question 8.1.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The eTD system will have system administrators who assign user roles. Documentation will be maintained within the eTD system stored in the ICE Electronic Library Management System. In addition, audit logs for the eTD system will capture information showing access of the system by specific users. These logs may be reviewed at any time to identify unusual activity that would indicate improper use, but may only be accessed by users with appropriate "need to know" administrative rights necessary to ensure user compliance with operating and privacy policies. ICE will conduct planned reviews of the audit logs on a quarterly basis. In addition, MOUs with foreign countries participating in the eTD program are 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 the eTD system. Audit logs will be maintained indefinitely.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

DHS ICE will perform quarterly audits of the eTD system to ensure that security and role integrity.

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

As noted in section 8.4, the eTD system will maintain audit logs. These logs will document all user actions within the system including access of the system by specific users. These logs may be reviewed at any time to identify unusual activity that would indicate improper use. ICE will conduct planned reviews of the audit logs on a quarterly basis. In addition, MOUs with foreign countries participating in the eTD program are to report immediately 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 the eTD system. Audit logs will be maintained indefinitely. Only appropriate administrative staff will be able to access the audit logs for the sole purpose of review the appropriateness of any user's use of the system.

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

ICE employs accessing the system have received privacy and system security training. No additional privacy training is provided as part of the eTD system. The eTD system is only a

new mechanism for processing hardcopy travel document requests. Users will follow historical "hardcopy" protocols.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. C&A is finalized as of the date of the completion of this Privacy Impact Assessment.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

With an internet application, there are inherent security risks. ICE has limited these risks by using reasonable physical, electronic, and procedural safeguards to appropriately protect the information maintained in eTD against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, or deletion. Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including the encryption of all personal identifying information and all other FOUO information held on portable media such as data tapes, CDs, or laptops.

In addition to the measures discussed above, the eTD System has built-in firewalls, limited accesses, segregated roles, and scheduled system audits. The audit logs capture access of the system by specific users.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The eTD System was built from the ground up by an independent contractor pursuant to ICE requirements. Persons whose information is contained in the system are neither lawful permanent residents nor United States citizens. Moreover, based on the proposed retention schedule, such persons are not able to become lawful permanent residents or United States citizens during the time their information is contained within the system. Therefore, this is not a system of records within the meaning of the Privacy Act, 5 U.S.C. § 552a.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data relating to the respective alien was gathered from the alien and/or from identity documents referring to the alien. Even prior to the development of the eTD, ICE collected biographic and biometric information relating to aliens ordered removed, and shared such information with foreign governments in order to secure travel documents. The ability to secure travel documents often depends on the accuracy of information collected on such aliens. ICE makes efforts to verify the information it collects by comparing it to other information in its possession. Where there is a discrepancy in agency data, ICE will conduct an interview with the alien in order to resolve such issues. The eTD System is a new electronic delivery mechanism for established procedures. Dedicated system user IDs and passwords, user role assignment and verification, and system firewalls are designed to provide secure access. ICE will use reasonable physical, electronic, and procedural safeguards to appropriately protect the information maintained in eTD against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, or deletion. Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including the encryption of all personal identifying information and all other FOUO information held on portable media such as data tapes, CDs, or laptops.

9.3 What design choices were made to enhance privacy?

The eTD system will systematically and periodically purge data from the system. This reduces the probability of an unauthorized access to information. ICE will use reasonable physical, electronic, and procedural safeguards to appropriately protect the information maintained in eTD against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, or deletion. Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including the encryption of all personal identifying information and all other FOUO information held on portable media such as data tapes, CDs, or laptops.

Conclusion

The electronic Travel Document was designed as means of making a paper-based procedure electronic for sharing basic identification information with foreign governments.

Users of the eTD system are segmented by individual roles, and there are firewalls, private networks, and physical segmentation of law enforcement data to prevent access of private/sensitive data from outside of the ICE infrastructure. The data is retained and governed by the same rules that apply with physical A-file storage, and data is kept on the eTD system for 90-day and 180-day intervals. The eTD system is certified and accredited with FISMA compliance.

Responsible Official(s)

Robert B. Shiflett
Office of Detention and Removal Operations
Immigration and Customs Enforcement
202-732-2931

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security