



**Privacy Impact Assessment Update
for the
Electronic System for Travel Authorization
(ESTA) Fee
DHS/CBP/PIA-007(a)**

July 18, 2011

Contact Point

**Suzanne Shepherd
Acting Director – ESTA
U.S. Customs and Border Protection
(202) 344-3710**

Reviewing Official

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



Abstract

U.S. Customs and Border Protection (CBP) is publishing this update to the Privacy Impact Assessment (PIA) for the Electronic System for Travel Authorization (ESTA) dated June 3, 2008.¹ ESTA is a web-based application and screening system used to determine whether certain aliens are eligible to travel to the United States under the Visa Waiver Program (VWP). This update will evaluate the privacy impacts of updating the login procedures, collecting an application fee, and adding the Pay.gov tracking number and country of birth information to the ESTA System of Records. Additionally, this update is to provide further notice of the expansion of routine sharing of ESTA with the intelligence community in support of the Department's mission to protect the United States from potential terrorist activities.

Introduction

In 2008, U.S. Customs and Border Protection developed and implemented the Electronic System for Travel Authorization (ESTA) to determine the eligibility of aliens to travel to the United States by air or sea under the VWP, prior to boarding a carrier en route to the United States, and whether such travel poses a law enforcement or security risk. Applicants submit their biographical information using the ESTA website, which makes a determination about the applicant's authorization to travel to the United States after performing screening and targeting against selected security and law enforcement databases, and lookouts using CBP TECS and the Automated Targeting System.

Authorized by Section 711(d)(1)(E) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-053, and required by the Travel Promotion Act (TPA), Pub. L. No 111-145, signed into law on March 4, 2010, CBP amended its regulations to include the collection of an administrative fee for the use of the ESTA system. In addition to the administrative fee, the TPA mandates that CBP collect \$10 from each VWP applicant that receives authorization under ESTA to travel to the United States. CBP must transfer these funds monthly to the Travel Promotion Fund for use by the Corporation for Travel Promotion.

Applicants use the ESTA web-based interface to provide the required information. When the user has entered all the required information and is ready to make payment, ESTA will take the applicant through a series of screens where he/she enters the billing name, billing address, and credit card information. ESTA forwards all of the information to Pay.gov for payment processing, and the applicant name and an ESTA tracking number to the CBP Credit/Debit Card Data System (CDCDS) for payment reconciliation. Pay.gov sends a nightly activity file, including the last four digits of the credit card, authorization number, billing name, address, ESTA tracking number, and Pay.gov tracking numbers, to CDCDS. Pay.gov also sends a daily batch file with the necessary payment information to Fifth Third Bank for settlement processing. After processing, Fifth Third Bank sends a settlement file, including the full credit card number,

¹ Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_esta.pdf



authorization number, card type, transaction date, amount, and ESTA tracking number to CDCDS. CDCDS retains the data from these transactions on different tables.

CDCDS matches the data transmitted from ESTA, Pay.gov, and Fifth Third Bank by the ESTA tracking number and posts payments to CBP's account. CBP uses the data in CDCDS to manually research and reconcile unmatched transactions to the proper account, and to research and respond to charge-backs by the applicant, if necessary.

CBP allows applicants to access their ESTA account to modify their travel itinerary information without incurring an additional fee. Applicants must provide their ESTA application number, date of birth, and passport number to update their ESTA information. If an applicant has forgotten their application number, the applicant will be able to retrieve the ESTA application number by providing their name, passport number, date of birth, and passport issuing country.

CBP anticipates collecting country of birth information to refine its ability to match, more efficiently, applicants with relevant information during the vetting process.

In addition to changes to the program, DHS has expanded its of routine sharing of ESTA with the intelligence community in support of the Department's mission to protect the United States from potential terrorist activities. Pursuant to the National Security Act of 1947, as amended, the National Counterterrorism Center (NCTC) "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." 50 U.S.C. § 404o. In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 27, 2005), which provides that the head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the head of each other agency that has counterterrorism functions. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (Pub. L. No. 108-458), as amended, places an obligation on U.S. government agencies to share terrorism information with the intelligence community. In certain instances, DHS shares the entire dataset with an intelligence community member in order to support the counterterrorism activities of the intelligence community and to identify terrorism information within DHS data. DHS has decided to share the entire ESTA database with NCTC under a Memorandum of Understanding (MOU). The MOU permits NCTC to use ESTA information to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. The MOU includes a number of safeguards to ensure the data is only used for the purposes explicitly permitted under the MOU, this PIA and the applicable SORN. The MOU also limits the amount of time the information is maintained at NCTC, ensures proper information technology security is in place during and after transmission of the ESTA data to NCTC, requires training for staff accessing ESTA, and provides for routine reporting and auditing of NCTC's use of the data.

Reason for the PIA Update

DHS/CBP is updating the existing PIA (DHS/CBP/PIA-007) first published on June 3, 2008 to account for the fee requirements of the TPA. CBP must collect a fee for the use of the



ESTA system: \$10 from each VWP applicant approved for travel to the United States, and an additional amount for the processing of an ESTA application which will ensure recovery of the costs to administer the ESTA Program (first authorized by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-053). CBP is implementing an access capability so that applicants may return to partially completed applications and update their travel itinerary information without incurring additional costs. CBP anticipates collecting country of birth information to refine its ability to match, more efficiently, applicants with relevant information during the vetting process.

Additionally, DHS/CBP is updating the ESTA PIA to account for the routine sharing of ESTA data with the intelligence community. DHS has entered into a MOU with the NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. DHS and NCTC have placed specific safeguards in this MOU to ensure that the data is used appropriately and in accordance with the existing system of records notice for ESTA (last published June 10, 2009 73 FR 32720) and this PIA.

Privacy Impact Analysis

Each of the below sections consider how the ESTA system has changed, and what impact it has on the below fair information privacy principles. In some cases there may be no changes to ESTA or to the resulting impact on the fair information privacy principles.

The System and the Information Collected and Stored within the System

Applicants use the ESTA web-based interface to provide both the required ESTA application information and payment information. When the user has entered all the required application information and is ready to make payment, ESTA will take the applicant through a series of screens where the traveler enters the payment information (billing name, billing address, and credit card information). CBP will use billing name, address, and credit card information only to process payments and resolve payment issues. Such payment information will not be used for vetting purposes, nor is it included in the information sharing with NCTC described in this update. To keep this payment information separate from the application, it will not be stored with application data in ESTA, but forwarded to Pay.gov and eventually stored in CDCDS. ESTA will collect and store the Pay.gov tracking number which it receives from Pay.gov to ensure the payment is associated with the correct ESTA application.

ESTA will forward payment information to Pay.gov for payment processing, and will forward the applicant name and an ESTA tracking number to the CDCDS for payment reconciliation. Pay.gov sends a nightly activity file, including the last four digits of the credit card, authorization number, billing name, address, ESTA tracking number, and Pay.gov tracking numbers to CDCDS. Pay.gov also sends a daily batch file with the necessary payment information to Fifth Third Bank for settlement processing. After processing, Fifth Third Bank sends a settlement file, including the full credit card number, authorization number, card type, amount, ESTA tracking number, and transaction date, to CDCDS. CDCDS retains the information from these transactions on different data tables.



ESTA anticipates collecting and storing country of birth information. The traveler's country of birth information will be requested in the ESTA application. This information will assist CBP in refining its ability to match, more efficiently, applicants with relevant information during the vetting process.

Uses of the System and the Information

CBP uses the payment information to ensure correct reporting to Treasury, for reconciliation, and to handle any payment issues (retrieval requests and charge-back pre-notifications). Pay.gov uses the payment information to pass to Fifth Third Bank for settlement processing.

Payment information obtained through the ESTA application process will not be used by CBP for vetting purposes, and is stored in a separate system (CDCDS) from the rest of ESTA application data. The ESTA tracking number will be used to assist CBP in reconciling accounts and payments where there is a discrepancy.

Applicants will now be able to log in to their ESTA account to modify their travel itinerary information without incurring an additional fee. If an applicant changes information in their account which alters their status under the VWP, the applicant may need to reapply under ESTA, and may be charged additional fees for reapplying.

Country of birth information provided to CBP will be used in refining CBP's ability to match, more efficiently, applicants with relevant information during the vetting process along with the rest of the ESTA application information.

Retention

National Archives and Records Administration (NARA) guidelines for retention and archiving of certain data will apply to ESTA. However, CBP is still in the process of seeking NARA approval for the ESTA data retention and archiving plan. CBP retains ESTA application data (including the country of birth information) for no more than three years in an active database (one year beyond the expiration date) and twelve years in archive status. Upon arrival in the United States, the information in the ESTA application is used to populate an I-94 Arrival/Departure record in the Non-immigrant Inspection System (NIIS). CBP retains Arrival/Departure records in NIIS for 75 years to support claims for benefits and requests to change status under the Immigration and Nationality Act (INA).

Payment information will be maintained in CDCDS for nine months in an active database to reconcile accounts, and six years and three months archived in conformance with NARA General Schedule 6 Item 1 Financial Records management requirements. The nine month active status is necessary to handle the majority of reconciliation issues (including charge-back requests and retrievals), which may be initiated by the applicant's bank up to 18 months after the transaction. CBP must respond to these issues within 10 to 15 days or lose the payment. Following the archived period, this information will be destroyed by deletion from CBP IT systems, unless it has become associated with a law enforcement activity, in which case it will be retained for the duration of that law enforcement activity and any related enforcement activities. This retention schedule is being reflected in the CDCDS SORN, which is being published in



conjunction with this PIA. Pay.gov will maintain the payment information for 7 years per their requirements for financial records (See 68 FR 5691).

With regard to information shared with NCTC, NCTC will be allowed to retain a defined subset of ESTA data for the same period of time as CBP maintains the information order to identify terrorism information, in support of its counterterrorism mission and in support of the mission of DHS. ESTA data will be deleted by NCTC no later than two years from receipt unless a nexus to terrorism has been identified for a particular record. NCTC may retain ESTA data containing terrorism information in accordance with NCTC authorities and policies, applicable law, and the terms of the MOU.

Internal Sharing and Disclosure

The payment information will be made available to CBP employees to process and reconcile payment issues. Country of birth information will be collected as part of the ESTA application process to determine the applicant's eligibility to travel to the United States under the VWP. CBP will continue to apply established protection procedures for ESTA information and any payment information, including the use of restricted roles and required privacy trainings for internal users, and periodic audits to achieve oversight.

External Sharing and Disclosure

CBP will now share payment information (billing name, billing address, and credit card) and the ESTA tracking number with Pay.gov and Fifth Third Bank for payment processing and payment reconciliation. CBP is amending its Systems of Records Notices (SORNs) routine uses to reflect this new sharing. Payment information will not be provided to the Department of State when the applicant has been denied an authorization to travel to the United States under the VWP. However, the country of birth information, along with the application data, will be forwarded to the Department of State in conjunction with a denial or approval of the ESTA. Payment and country of birth information will not be sent to the carriers, though a failure to provide payment will result in a "not authorized to travel" message to the carrier via APIS/AQQ.

The information submitted by the applicant in the ESTA application (excluding the payment information) is used for vetting and may be shared, on a need to know basis, with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement or intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. All transmissions of this information will be over secure electronic connections or as printed materials to authorized personnel.

In addition, DHS has entered into a new sharing agreement with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. This sharing is conducted pursuant to routine use L of the ESTA SORN, which states that DHS may share ESTA information with a "Federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably



believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.”

NCTC will be allowed to retain all ESTA records that do not constitute terrorism information for two years from receipt. This process will be audited as required under the MOU. DHS/CBP will not share payment information with NCTC as part of the routine exchange of ESTA records. NCTC will review, retain, and disseminate ESTA records it has determined have a nexus to terrorism in accordance with procedures approved for NCTC by the Attorney General in accordance with Section 2.3 of Executive Order 12333 and additional terms specified in the MOU.

The MOU has strict safeguards to protect the PII provided to NCTC. These protections include a routine oversight of NCTC’s use of the data by DHS personnel detailed to NCTC. In addition, training has been provided to NCTC users on the appropriate use of personally identifiable information. DHS/CBP will provide annual and periodic training to appropriate NCTC personnel on proper interpretation of the data contained in ESTA and on proper treatment of data from certain categories which require special handling, such as asylum, refugee, and U.S. Person data.

NCTC may not disseminate to third parties information derived from ESTA data, unless that data was identified as containing terrorism information. NCTC shall maintain an electronic copy and accounting of the APIS data that was disseminated, to whom, and the purpose for the dissemination.

Additionally, this external sharing, outside of DHS, is being appropriately logged pursuant to subsection (c) of the Privacy Act, which requires the Department to maintain a log of when records have been shared outside of DHS. In accordance with the system of records notice for ESTA, DHS has exempted this accounting for disclosure required by subsection (c) from the access provisions of subsection (d).

Notice

CBP published updated regulations on August 9, 2010 (75 FR 47701), is publishing this update to the ESTA PIA and will be publishing updated SORNs to inform the public about the collection, use, and disclosure of information submitted by applicants in conjunction with the ESTA application. Additionally, applicants visiting the ESTA website are notified of the required fees and data elements on the website.

Individual Access, Redress, and Correction

CBP is providing secure access for applicants so that they may correct and view their travel itinerary information. This access requires the user to have information that should only be in the possession of the applicant or someone authorized to act on the applicant’s behalf, such as the applicant’s passport number and ESTA application number.

Under the Privacy Act and Freedom of Information Act (FOIA) individuals may request access to the information they provide which is maintained in the applicable CBP system of records, including any payment and/or country of birth information. Proper written requests under the Privacy Act and FOIA should be addressed to:



U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue, NW
Washington, DC 20229

Further, individuals will now have the ability to access their ESTA information in order to make appropriate corrections or view the information they previously provided with respect to their active ESTA data.

Applicants denied a travel authorization to the United States via ESTA may apply for a visa from the U.S. Department of State. General complaints about treatment or requests for redress can be made to the DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Generally, if a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to:

CBP INFO Center
OPA - CSC - Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Ave, NW
Washington, DC 20229
Phone - (877) 227-5511

Technical Access and Security

To provide additional security for those applicants who have lost or do not know their ESTA application number, CBP will only provide this information if the user is able to provide the applicant's name, passport number, date of birth, and passport issuing country. Once this information has been provided, CBP will allow the user to retrieve his/her application number.

DHS/CBP Internal user access to data in ESTA is controlled through passwords and restrictive rules pertaining to user rights. Internal users are limited to roles that define authorized use of the system. Procedural and physical safeguards are utilized such as accountability audits, receipt records, and site security. Management oversight is in place to ensure appropriate assignment of roles and access to information.



Technology

CBP is employing no new technology aside from the software that provides a secure log in for applicants and connections to Pay.gov and Fifth Third Bank for payment processing.

Responsible Officials

Suzanne Shepherd, Acting Director – ESTA
U.S. Customs and Border Protection
Department of Homeland Security

Laurence E. Castelli
CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer,
Department of Homeland Security.