Privacy Impact Assessment
for the

Electronic System for Travel Authorization

(ESTA)

June 2, 2008

Contact Point:
Beverly Good
Director, Admissibility and Passenger Programs--ESTA
Customs and Border Protection
(202) 344-2433

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

CBP is issuing an Interim Final Rule to create regulations governing the submission of Electronic System for Travel Authorization (ESTA) data, a new system of records notice, and an associated Privacy Impact Assessment (PIA). The ESTA regulations will govern the collection and use of personally identifiable information in determining the eligibility to travel of persons seeking to enter the United States under the Visa Waiver Program (VWP) by air or sea. The regulations will require nationals of VWP countries seeking to enter the United States by air or sea carriers to submit personally identifiable information to an electronic system, ESTA, prior to travel. ESTA will run the applicant's information against various databases to determine whether there is a law enforcement or security reason to deem that a prospective traveler is ineligible to travel to the United States under the VWP. The ESTA system will serve to modernize and strengthen the security of the VWP as mandated by the "Implementing Recommendations of the 9/11 Commission Act of 2007" (9/11 Act), by providing automated vetting of travelers from VWP countries.

Introduction

On August 3, 2007, the President signed the 9/11 Act into law. Section 711 of the 9/11 Act, entitled Modernization of the Visa Waiver Program (VWP), provides for the expansion and enhancement of the VWP program. Included in Section 711 is the requirement for the Department of Homeland Security (DHS) to develop a fully automated system, known as Electronic System for Travel Authorization (ESTA), that would 1) require foreign nationals of VWP countries to apply for and secure advance authorization to travel to the United States by air and sea under VWP, and consequently 2) afford DHS the opportunity to fully screen (vet) the applicant to determine their eligibility to travel to the United States under the VWP. The modernization and expansion provisions of the 9/11 Act apply to the current slate of VWP countries and will apply to the 13 so-called "Roadmap" countries that are currently under consideration for inclusion in the VWP. The Roadmap countries that are under consideration for inclusion within the VWP include Bulgaria, Cyprus, Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia and South Korea.

During FY2006, the 27 countries that currently participate in the VWP accounted for 15 million visits to the United States. If the VWP were expanded to include all 13 Roadmap countries, travel to the United States could expand by an estimated additional three million VWP travelers annually.

System Overview

As mandated by Congress, DHS must deploy a fully automated electronic travel authorization system. In support of this requirement, CBP is developing a system that includes an internet-based application and attendant vetting mechanism that will accommodate the entry of information (i.e.,

the "ESTA Application") by the ESTA applicant, the vetting of the application by DHS, and the return notification indicating "authorized to travel" or "not authorized to travel" to the applicant, both via update to the application on the internet site. If additional time is needed to determine the applicant's eligibility, the return notification will display a "pending" status and may be accessed later through a unique tracking number in combination with some personally identifiable information (for example, date of birth and passport number).

Prospective travelers from the designated VWP countries seeking to enter the United States by air or sea will be required to apply for ESTA via the internet-based ESTA application prior to their travel to the United States. The applicant must comply with the following requirements:

- Submission of all information requested on the ESTA application
- Attestation that the information submitted is accurate
- Provision of an electronic signature

Applicants will be advised to comply with the above requirements at least 72 hours before departure. Vetting of the applicant/application will be accomplished typically through interfaces with CBP's existing systems for screening passengers and determining admissibility.

Upon receipt of an ESTA application, CBP will examine the application by screening the applicant's data through law enforcement systems, including the Automated Targeting System[1] (ATS) (to screen for terrorists or threats to aviation and border security) and the Treasury Enforcement Communications System[2] (TECS) (for matches to persons identified to be of law enforcement interest).

When the vetting process identifies a situation wherein authorization to travel should be withheld, appropriate indication of a denial will be returned to the applicant via the ESTA website. Denials will result in a notice to the applicant that the authorization to travel under the VWP will not be granted and will refer the applicant to the Department of State's website for information on how to apply for a visa at a United States embassy or consulate. Denials, including the application data and result, will be forwarded to the Department of State to assist in determining the applicant's eligibility for visa issuance.

[1] SORN at 72 *Fed. Reg.* 150 (6 August 2007). PIA available online at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf
[2] SORN at 66 *Fed. Reg.* 202 (18 October 2001).

An official determination of an applicant's ESTA status of authorized to travel will be provided to the carriers to permit transportation only of those individuals who have been authorized by ESTA to travel under the VWP program or have a visa. The carriers will be notified through the Advance Passenger Information System Quick Query (APIS/AQQ) Program when the carriers initiate an interactive APIS/AQQ query. Carriers will be notified through this system whether the passenger has an authorized ESTA, has not applied for an ESTA, or requires a visa. Applicants denied an ESTA will be required to apply for a visa at a U.S. consulate or embassy where redress issues will be handled.

In conjunction with CBP's final rule "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," which was published in the Federal Register on August 23, 2007 (and became effective on February 19, 2008), DHS has been coordinating with commercial aircraft and commercial vessel carriers on the development and implementation of messaging capabilities for passenger data transmissions that will enable DHS to provide the carriers with messages pertaining to a passenger's boarding status. A prospective VWP traveler's ESTA status is a component of a passenger's boarding status that has been introduced into the plans for implementing messaging capabilities between DHS and the carriers.

The development and implementation of the ESTA program will eventually allow DHS to eliminate the requirement that VWP travelers complete an I-94W prior to being admitted to the United States. Upon ESTA becoming mandatory, a VWP traveler with valid ESTA will not be required to complete the paper Form I-94W when arriving on a carrier that is capable of receiving and validating messages pertaining to the traveler's ESTA status as part of the traveler's boarding status.

Section 1.0
Information collected and maintained

The following questions are intended to define the scope of the information requested as well as 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 ESTA Application will require individuals to provide the following data elements, similar to those requested by the I-94W:

- Last name, First and Middle Names
- Unique ESTA identifier (provided by CBP)
- Email Address, if available
- Phone Number
- Date of Birth
- Country of Citizenship
- Sex
- Passport Expiration Date
- Passport Number and Issuance City , Country, and Date

- Destination Address, City, State
- Flight Information, if available
- City of Embarkation, if available
- Whether the individual has a communicable disease, physical or mental disorder, or is a drug abuser or addict?
- Whether the individual has been arrested or convicted for a moral turpitude crime, drugs, or has been sentenced for a period longer than five years?
- Whether the individual has engaged in espionage, sabotage, terrorism or Nazi activity between 1933 and 1945?
- Whether the individual is seeking work in the United States?
- Whether the individual has ever been denied a United States visa or entry into the United States or had a visa cancelled? (If yes, when and where?)
- Whether the individual has been excluded or deported, or attempted to obtain a visa or enter the United States by fraud or misrepresentation?
- Whether the individual has ever detained, retained, or withheld custody of a child from a United States citizen granted custody of the child?
- Whether the individual has ever asserted immunity from prosecution?

The ESTA application will store this information within the applicant's "account" along with an individual tracking number.

The information provided by the individual will be screened against the Automated Targeting System (ATS) (to screen for terrorists or threats to aviation and border security) and the Treasury Enforcement Communications System (TECS) (for matches to persons identified to be of law enforcement interest), and will automatically result in an "authorized to travel", "not authorized to travel", or "pending" status. "Pending" will be resolved to "authorized" or "not authorized" based on further research by CBP.

1.2 From whom is information collected?

The requirement to obtain a travel authorization under the ESTA program applies to citizens of VWP countries who are seeking to enter the United States under the VWP by air and sea. This includes those travelers without a valid unexpired U.S. visa and seeking to enter the United States for the purpose of business or pleasure for 90 days or less. Upon full implementation of ESTA, all aliens traveling under the VWP by air or sea will be required to obtain ESTA authorization before embarking on a carrier for travel to the United States. All aliens participating in the VWP must submit this information before embarking on an air or sea carrier for travel to the United States. In situations where a third party (e.g., a relative or travel agent) provides the information on behalf of the applicant, that third party will not be required to provide any personally identifiable information about him or herself.

Countries currently participating in the VWP:

1. Andorra
2. Australia
3. Austria

4. Belgium
5. Brunei
6. Denmark
7. Finland
8. France
9. Germany
10. Iceland
11. Ireland
12. Italy
13. Japan
14. Liechtenstein
15. Luxembourg
16. Monaco
17. Netherlands
18. New Zealand
19. Norway
20. Portugal
21. San Marino
22. Singapore
23. Slovenia
24. Spain
25. Sweden
26. Switzerland
27. United Kingdom

Proposed Roadmap countries:
1. Bulgaria
2. Cyprus
3. Czech Republic
4. Estonia
5. Greece
6. Hungary
7. Latvia
8. Lithuania
9. Malta
10. Poland
11. Romania
12. Slovakia
13. South Korea

1.3 Why is the information being collected?

As required by Section 711 of the 9/11 Act, DHS is collecting the information under ESTA to determine the eligibility of aliens to travel to the U.S. 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. The data elements contained on the application are largely the same as that collected via the I-94W Nonimmigrant Alien Arrival/Departure Form (I-94W) and DHS has determined are necessary to implement the ESTA provision under Section 711 of the 9/11 Act.

1.4 How is the information collected?

ESTA will allow prospective and repeat travelers from VWP countries to apply for and check the status of their authorization to travel under the VWP via a secure website.

- DHS advises that travelers obtain ESTA authorization at least 72 hours prior to embarkation for travel to the U.S., to allow for time for alternative arrangements in the event of ESTA denial.
- Applicants must fill out and submit an online form with the required information.
- The applicant will review the ESTA requirements and disclaimers prior to completing the application.
- The applicant will provide the required biographic and admissibility data listed above on the electronic form, confirm that the information provided is true and accurate, and submit this information through the ESTA website.
- Once the applicant has submitted their information, they will be given a unique tracking number. This tracking number, in combination with some personal data element(s) provided by the applicant in their application, can be used by the applicant to log in to the ESTA website to view or update the information they submitted, as well as check on the status of their ESTA application.
- Only the destination address in the United States, carrier, flight number, city of embarkation, email and telephone number may be updated for applicants that have already submitted their information. Changes to any of the other data elements will require the applicant to submit a new ESTA application, because these changes may affect the applicant's admissibility or reflect a change in the applicant's ability to travel under the VWP.
- ESTA authorization will be valid for a period of two years from approval or for a shorter period time in situations where a traveler's passport will expire less than two years from the date of ESTA authorization.

Once the form is completed, the information is transmitted through the automated system, which vets and maintains the applicant's information. The automated system will provide back a response of "authorized to travel," "pending," or "not authorized to travel." Where the status is reported as pending, the applicant will need to return to the site at a later time to obtain information concerning the resolution of his or her application. Where an applicant has been denied an ESTA, he or she will be directed to seek a visa from a United States consulate or embassy, from which additional redress options will be available.

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

Section 711 of the 9/11 Act provides for the expansion and the enhancement of the VWP. Pursuant to the 9/11 Act, Congress mandated that the Secretary of Homeland Security develop a fully automated electronic travel authorization system to determine, in advance of travel, whether a prospective VWP traveler is eligible to travel to the United States under the VWP and whether such travel poses a law enforcement or security risk.

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

Applicants for an ESTA are required to provide no more information than that which is already submitted on the I-94 W, Notice of Arrival/Departure. Overtime the ESTA will replace the need for the paper I-94 W to be submitted. The applicant's web-based submission will be protected by encrypted transport layered security; travelers will be instructed to keep personal information (such as a passport number) and the tracking number separate. ESTA accomplishes this by putting the tracking number on a separate page from the application, and further encouraging the applicant to retain the tracking number separate from his or her passport.

In filling out the online form, CBP recognizes that some individuals may be more comfortable having a third party supply the information or fill out the ESTA application on their behalf. In these cases, CBP assumes the applicants are aware that they will be providing personally identifiable information to third parties and consent to these third parties' access to the information. In these instances, the ESTA application will require an affirmative acknowledgment by the third party, who is entering the data, that the third party has received consent from the applicant to complete the ESTA. If an applicant cannot provide the requisite information through ESTA, the applicant must obtain a visa from a U.S. consulate or embassy before traveling to the United States.

Section 2.0
Uses of the system and the information

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

2.1 Describe all the uses of information.

DHS will use the information collected through ESTA to determine whether allowing the applicant to travel to the U.S. poses a law enforcement or security risk to the United States. Specifically, ESTA will vet non-immigrant applicants who wish to travel to the United States under the VWP for

national security, law enforcement, lost and stolen passport, visa cancellation and revocation, and VWP eligibility purposes. CBP will use the information entered by the applicant via the ESTA system to:

1) Forward the information to the mechanized CBP Vetting application to determine whether the individual is from a VWP country.
2) Run the applicant's data against Terrorist Screening Database (TSDB) biographical records, Interpol lost and stolen passport records, and Department of State's lost and stolen passport records and visa revocations to determine whether the applicant poses a law enforcement or security risk in traveling to the United States.
3) Store the application and vetting result (authorized to travel, pending, not authorized to travel) within the Applicants "account" for subsequent summarization, CBP/DHS management reporting, and limited updates by the applicant.
4) Forward the application to the CBP National Targeting Center (NTC) for further vetting if derogatory information appears.
5) Return communication to the Applicant of results of the application (authorized to travel, pending, not authorized to travel) via the ESTA website.
6) Forward the application to Department of State systems in the event the application is denied.
7) Forward the completed application result (authorized to travel, pending, not authorized to travel, or no application received) to the APIS/AQQ system for subsequent carrier verification of ESTA or visa.
8) Verify information on the ESTA application during examination by CBP Officers at Ports of Entry.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. The ESTA system does not analyze any data, but rather does name matching and screening using existing DHS IT systems. CBP will examine the application by screening the applicant's data through the Automated Targeting System[3] (ATS) (to screen for terrorists or threats to aviation and border security) and the Treasury Enforcement Communications System[4] (TECS) (for matches to persons identified to be of law enforcement interest).

[3] SORN at 72 *Fed. Reg.* 150 (6 August 2007). PIA available online at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf
[4] SORN at 66 *Fed. Reg.* 202 (18 October 2001).

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

The individual or his/her designee submits the information directly to DHS through the online ESTA form. Click-through windows and other advisory notices will be provided on the application requiring ESTA applicants to acknowledge reading and understanding the information required and the privacy policy. Applicants will be further notified that their ESTA will only remain valid so long as the information (other than the travel information related to the particular travel, such as destination city, flight information, and city of embarkation) they supplied is correct and current. The individual or his/her designee is required to certify the information. After submission, the applicant's information is checked for accuracy by airline personnel during the check-in process and again by Customs and Border Protection officers when the individuals present themselves for inspection at the port of entry. The individual's biographic and passport information will be compared to information submitted on the ESTA to verify its accuracy. In the event the applicant presents themselves at a U.S. embassy or consulate to apply for a visa, DOS will verify the identity of the applicant against the information provided by ESTA and proceed to process the visa application using DOS vetting procedures.

To ensure the applicant's information is timely and accurate, information will be posted on the ESTA program website and will provide applicants limited access to their account for updates to their destination address in the United States, carrier, flight number, city of embarkation, email and telephone number.

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

While the information collected is the same as the I-94W, this collection is for the limited purpose of determining whether allowing the applicant to travel to the United States poses a law enforcement or security risk to the United States. ESTA will not determine whether the traveler is, in fact, admissible to the United States without a visa as this function will continue to be performed by a CBP officer following inspection at a port of entry. Having the applicant fill out the ESTA application online ensures accuracy, because the applicant is in the best position to supply accurate information and verify its accuracy as it is submitted. Over time, the ESTA will replace the paper I-94W and as such, will then follow the uses associated with the I-94W data.

ESTA is a two-tiered system that divides access to internal and external users. External users consist of the applicants, eligible to travel under the VWP and their agents. Internal users consist of CBP/DHS personnel with authorized access to the ESTA system.

External Users:

External users can only input PII into ESTA through the website, they cannot extract PII. Applications are blank, even for updates to accounts, so that third parties cannot log in and gain access to an applicant's data through a pre-populated screen. While the nature of the ESTA website permits a third party to enter the information into the system on behalf of the applicant, CBP assumes that the applicant has consented to the third party's access to their PII.

Applicant information retained in the applicant's ESTA account will be protected from external users gaining unauthorized access by requiring a unique tracking number in combination with the applicant's date of birth and passport number. Because the information contained in the passport is not enough to access the ESTA account, someone who has stolen a passport without also obtaining the tracking number will not be able to log in and access the applicant's PII or check the status of the applicant's ESTA. Applicants will be advised to keep their passport and tracking number separate. Further, data will be encrypted using the NIST approved transport layered security data encryption technology at the interface level to prevent third parties from monitoring or accessing an applicant's PII when filling out and submitting an application.

Where inaccurate information results in an applicant being denied an ESTA, the applicant will be directed to a U.S. embassy or consulate to resolve the issue and apply for a visa, if appropriate.

Internal Users:

To mitigate the risk of misuse of information by DHS employees and contractors with access to ESTA, 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 and receipt records. Management oversight is in place to ensure appropriate assignment of roles and access to information.

In order to become an authorized internal user, personnel must successfully complete privacy training and hold a full field background investigation. An internal user must also have a "need-to-know" the specific information. Additionally, because ESTA will use some aspects of the Advance Passenger Information System (APIS), which resides on the TECS IT platform, all internal users of the ESTA system are required to complete and pass an annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy as they are presented. An internal user must pass the test scenarios to retain access to TECS and more specifically, ESTA. This training is regularly updated.

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?

ESTA authorizations generally expire and are deemed "inactive" two years from the date of approval. In the event that a traveler's passport is valid for a period of time less than two years from the date of ESTA authorization, it is anticipated the ESTA authorization will be valid for the period of time that the traveler's passport is valid. Information in ESTA will be retained for one year after the ESTA expires. After this period, the inactive account information will be purged from online access and archived for 12 years. However, data linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including applications for ESTA that are denied will remain accessible for the life of the law enforcement activities to which they may become related.

As noted above, the ESTA application data will over time replace the paper I-94W form. In those instances where an ESTA is then used in lieu of a paper I-94W, the ESTA will be maintained in accordance with the retention schedule for I-94W, which is 75 years.

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

No. NARA guidelines for retention and archiving of data will apply to ESTA and CBP is in negotiation with NARA for approval of the ESTA data retention and archiving plan.

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

ESTA authorizations are valid for no more than two years. Information is required to be retained in ESTA for as long as the traveler is authorized to travel to the United States to screen prospective travelers from Visa Waiver Program (VWP) countries as to whether a law enforcement or security risk exists in permitting VWP applicants to travel to the United States under the VWP. This information is retained for an additional year to permit CBP to extend the expiration date of an ESTA to a maximum of three years, should it choose to do so. Information is kept in archives for an additional 12 years to allow retrieval of the information for law enforcement and investigatory purposes. This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress.

As noted above, the ESTA will over time replace the paper I-94W form. In those instances where an ESTA is then used in lieu of a paper I-94W, the ESTA will be maintained in accordance with the retention schedule for I-94W, which is 75 years. I-94W and I-94 data are maintained for this period of time in order to ensure that the information related to a particular admission to the United States is available for providing any applicable benefits related to immigration or other enforcement purposes.

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?

Online web access to ESTA will be available to CBP only. However, the information collected by and maintained in ESTA may be shared with all component agencies within DHS on a need to know basis consistent with the component's mission. Access to ESTA information within DHS is role-based according to the mission of the component and the user's need to know in performance of his or her official duties.

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

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

4.3 How is the information transmitted or disclosed?

Information submitted by applicants for ESTA will be electronically transmitted via an internet based web portal to the CBP component systems upon submission using NIST approved transport layered security data encryption. ESTA will communicate with other CBP systems by using CBP's secure message interfaces with message traffic exchanged over routed and point-to-point network facilities.

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

To combat the inappropriate use of PII, information is shared only with DHS personnel who have a need to know the information as part of the performance of their official employment duties. Internal DHS access to ESTA data is controlled by CBP through the use of strict access controls for the users, passwords, background checks for individuals accessing the data, as well as system

audits that track and report on access to the data. Additionally, any individual with access has gone through proper privacy training.

For example, CBP officers performing secondary inspections at Ports of Entry (POE) will access ESTA to confirm identity and authorization to travel to the U.S. ESTA access is enabled via secure CBP LAN facilities at POE locations. CBP security procedures that govern the use/access of information housed within the CBP infrastructure are applicable for ESTA access and use of ESTA data. Internal access controls include strong password (employing capitals, numbers, and multiple characters), encryption and logging and review of all transactions. ESTA has been determined to be a major application and has been added to the DHS inventory. ESTA will be certificated and accredited using DHS and CBP guidelines

PII will automatically be forwarded to the CBP NTC for further vetting only when some derogatory information appears as a result of ESTA's queries against the listed systems.

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?

Information submitted during an ESTA application may be shared under a memorandum of understanding (MOU) with consular officers of the Department of State (DOS), to assist consular officers in determining whether a visa should be issued to the applicant after an ESTA application has been denied. Carriers will also receive the information regarding the applicant's ESTA via the APIS/AQQ system. Additionally information may be shared with appropriate Federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, or where DHS believes the information would assist enforcement of civil or criminal laws. Additionally, information may be shared when DHS reasonably believes such use is to assist in anti-terrorism efforts or intelligence gathering related to national or international security or transnational crime.

5.2 What information is shared and for what purpose?

All data collected by ESTA about an applicant will be shared with DOS to assist in adjudicating visa applications. All of the information submitted by the applicant 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

intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders.

When air carriers query the applicant through the APIS/AQQ system, ESTA will disclose whether the applicant has been authorized to travel, pending, not authorized to travel, or that no application has been submitted for the applicant.

5.3 How is the information transmitted or disclosed?

An applicant's information stored in ESTA will be automatically available to the DOS component systems if the application is denied, so that DOS may use the information submitted to determine whether a visa should be issued to the applicant. These electronic transmissions will be over secure CBP to DOS network connections that comply with applicable security guidelines and embodied in a memorandum of understanding (MOU).

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

Data sent to air carriers will be transmitted via the secure APIS/AQQ electronic portal, subject to the APIS/AQQ SORN requirements and the ISA requirements with the carriers.

Lastly, information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the Chief of the Privacy Act Policy and Procedures Branch, Regulations & Rulings, Office of International Trade, CBP, and will only be granted where the request and use are consistent with the Privacy Act, the published routine uses for ESTA, and the receiving agency agrees not to further share the information outside the receiving agency without the express written approval of CBP All three requirements—use consistent with purpose for collection, sharing consistent with a statutory or published routine use, and acceptance of the restriction barring unauthorized dissemination outside the receiving agency—and the legal responsibility clause for wrongful dissemination contained in the Paperwork Reduction Act (44 U.S.C. section 3510) are stated conditions to the receiving agencies acceptance and use of the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

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) and related Interconnection Security Agreement (ISA) will control the information sharing arrangement with DOS. The agreement will reflect the scope of protection and use of ESTA data by DOS and, in general, will follow the same privacy protection guidance as is in place for DHS and its components. ISAs with the carriers will reflect the change in the use of the APIS/AQQ electronic portal to notify the carriers of the following conditions as they pertain to individual passengers: (1) Authorization to travel, (2) Not Authorized to travel, (3) Pending, or (4) No Application Received - Authorization Denied.

5.5 How is the shared information secured by the recipient?

External organizations will secure ESTA information in a manner that is consistent with the practices that CBP has put into place, and CBP will memorialize these security practices in any MOUs or ISAs governing the sharing of ESTA information. Under the terms of these MOU and ISAs, DOS, other agencies, and the carriers will secure ESTA information consistent with their security practices that largely duplicate that which is in place for DHS. Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside the ESTA program other than as authorized by DOS to view such data during the consideration of granting a visa. Recipients from other agencies and carriers will be required by the terms of the information sharing agreement to employ security features to safeguard the shared information.

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

CBP requires through its MOUs that all non-CBP users with access to ESTA receive training regarding the safeguarding, security, and privacy concerns relating to information stored in ESTA. In the anticipated MOU with DOS, DOS will be required to certify that its systems users are required to be adequately trained regarding information security and to adhere to the same legal requirements for the protection of PII.

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

When sharing information with third parties, the same requirements related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the interface request and the implications on privacy related concerns are two factors that are included in both the initial and ongoing authorization, the written arrangement (MOU) and Interconnection Security Agreement ("ISA") that is negotiated between CBP and the external agency that seeks access to CBP data. The written arrangement specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. The ISA specifies the data elements, format, and interface type to include the operational considerations of the interface.

The written arrangements and ISAs are periodically audited and reviewed by CBP and the outside entity's conformance to the use, security, and privacy considerations is verified before Certificates to Operate are issued or renewed.

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?

Notice is provided to the individual at the time of the electronic collection on the website. If an individual has asked a third party to enter the information, the third party is provided the notice and is required to obtain the consent of the individual before entering the information. In addition, DHS is publishing an Interim Final Rule, a Privacy Act System of Records Notice in the Federal Register and a PIA describing the new system. ESTA is a new electronic collection of the listed information, and notice will be given to the public through the ESTA SORN in conjunction with this PIA, as well as in real time during an applicant's use of ESTA. Appropriate notice regarding the data to be collected and the requirement to attest to the accuracy of the data will be included in the information provided via the ESTA web-site.

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

No. Information must be provided pursuant to applicable statutes for all persons on covered air and sea carriers. An individual who declines to provide information necessary to complete an ESTA application will not be permitted to travel to the United States under the VWP. The only legitimate means of declining to provide the subject information is to choose not to travel the United States or to apply for a visa at a U.S. consulate or embassy.

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, individuals do not have the right to consent to particular uses of the information. Individuals may only choose whether or not they will submit their information in order to travel to the United States under the VWP. Once an individual submits the data for ESTA purposes, he or she cannot exert control over it, aside from his or her ability to amend specific data elements (i.e., destination address in the United States, carrier, flight number, city of embarkation, email and telephone number) by accessing his or her account and submitting these data elements.

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

There is a risk that individuals will not know that they are required to provide ESTA data. Adequate notice and disclaimer information, including the consequences of not providing the information requested, will be provided to the applicant and an indication of consent will be obtained before any information is collected. Explanation of the use of data will also be provided to the applicant on the website.

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?

Individuals whose personal information is collected and used by the ESTA program will not have access to their information through the ESTA web-site after submitting their ESTA application. Applicants will be able to see the information they supply on the application as they fill it out and again before submission, to confirm it is timely and accurate. Applicants will not be able to view any data once it has been submitted, because the web interface cannot guarantee the person requesting information is authorized to access it. After submission, applicants may update their accounts by submitting the new destination address in the United States, carrier, flight number, city of embarkation, email address or telephone number. Corrections to any other data elements will require the applicant to fill out and submit a new ESTA. Applicants that are denied authorization for travel to the United States will be directed to a U.S. embassy or consulate for a visa application. Should there be inaccuracies identified in the applicant's information during the visa application process, DOS will consider that fact in determining eligibility for a visa.

DHS allows persons, including foreign nationals, to seek access under the Privacy Act to certain information maintained in ESTA. Requests for access to personally identifiable information contained in ESTA may be submitted to the Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511). However, information maintained in ESTA pertaining to the accounting of a sharing with a law enforcement or intelligence entity in conformance with a routine use may not be accessed, pursuant to 5 U.S.C. § 552a (j)(2) or (k)(2). Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Individuals and foreign nationals may also seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through TRIP. TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through TRIP, a traveler can request correction of erroneous data stored in ESTA and other data stored in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

7.2 What are the procedures for correcting erroneous information?

Information erroneously submitted by applicants to ESTA can be corrected by the applicant via the ESTA web-site by making limited updates to their information or by creating a new ESTA. A CBP Officer may also administratively update the same fields as the applicant when he or she applies for admission to enter the United States at a port of entry. The CBP Officer will verify documentation presented by the traveler by comparing it against information entered in ESTA and determine whether the application can be administratively updated. Individuals whose personal information is collected and used by the ESTA program may, to the extent permitted by law, examine their information and request correction of inaccuracies. Individuals who believe ESTA holds inaccurate information about them, or who have questions or concerns relating to personal information and ESTA, may contact the ESTA Program Privacy Coordinator (See supra, 7.1).

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

Upon beginning an ESTA application, advisory notice and instructions will be provided via the ESTA web-site regarding the application process. Individuals will also be notified through the website and System of Records Notice of the availability of the ESTA Program Privacy Coordinator.

7.4 If no redress is provided, are alternatives available?

Yes, in addition to the above described redress procedures and options, individuals may also apply for a visa at a U.S. consulate or embassy.

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.

Individuals are not given access to their information via the ESTA web interface to guard against third parties accessing the applicant's PII. The ESTA application is for a determination of eligibility for travel under VWP, and the application is being submitted only for that determination. Once an applicant has submitted information and has been issued a grant or denial, the applicant cannot seek appeal of the determination through ESTA. Rather, the applicant may either correct erroneous information through the measures above, or apply for a visa at a U.S. consulate or embassy where redress will be handled in the form of granting or denying a visa for travel to the United States.

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? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Applicants under the VWP and other external users will not have access to the ESTA system beyond the ability to create accounts, update their account information, and submit applications. Access to the system for internal users is limited to a need to know basis. All internal users with access to the system are required to have full background checks. All program managers, IT specialists, and analysts and CBP Officers, the latter assuming authorization by the ESTA Security Administrator, will have general access to the system. DHS contractors, in particular those involved with systems support, will also have access to the system.

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.

Contractors to DHS may have an essential role in designing, developing, implementing, and managing the system due to their specialized expertise. Contractors must complete CBP full field background investigations before they are allowed to access any ESTA data and will also receive the same security and privacy training as CBP government employees. A copy of the contract will be submitted to the Privacy Office with this PIA.

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

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

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

The personal information collected and maintained by ESTA will be accessed principally by certain employees of DHS components and DOS consular officers. The ESTA program will secure information and the systems on which that information resides, by complying with the requirements of the DHS IT Security Program Handbook. This handbook established a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules. In order to gain access to the ESTA information, a user must not only have a need to know, but must also have an appropriate background check and completed annual privacy training. A supervisor submits the request to the Office of Information Technology (OIT) at CBP indicating the individual has a need to know for official purposes. OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems.

The MOUs and ISAs with DOS, other agencies, and the carriers specify security and access privileges. The agreements reflect the scope of protection and use of ESTA data by third parties (including other agencies) to follow the same privacy protection guidance as DHS employees.

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

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including ESTA. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Rules of behavior will be posted online prior to login for internal users. In addition, the rules of behavior already in effect for each of the component systems on which ESTA draws will be applied to the program, adding an additional layer of security protection.

Security, including access related controls, will be certified initially and at specified intervals by the CBP Security organization through Certification and Accreditation (C&A) of the ESTA system.

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

ESTA resides on its own platform, and transactions are tracked and monitored. This allows for oversight and audit capabilities to ensure that the data are being handled consistent with all

applicable laws and regulations regarding privacy and data integrity. ESTA maintains audit trails or logs for the purpose of reviewing internal and external user activity. ESTA actively prevents access to information for which a user lacks authorization as defined by the user's role in the system, location of duty station, and/or job position. Multiple attempts to access internal information without proper authorization will cause ESTA to suspend access automatically. Misuse of ESTA data can subject a user to discipline in accordance with the CBP Code of Conduct, which can include being removed from an officer's position. CBP Security will also use the logs during C&A activities to audit their completeness prior to issuing a certificate to operate.

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

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

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

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

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

Yes. ESTA is undergoing the Certification and Accreditation (C&A) process in accordance with DHS and CBP policy, which complies with these Federal statutes, policies, and guidelines, and will be certified and accredited prior to operation for a three year period as amended or when a major change is made to the system.

8.9 Privacy Impact Analysis: Given access and security

controls, what privacy risks were identified and describe how they were mitigated.

CBP identified privacy risks with respect to appropriate use and access to the information. These risks are mitigated through training, background investigations, internal system audit controls, the CBP Code of Conduct and Disciplinary system, and the practice of at least privileged access.

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 ESTA system is a stand-alone application that communicates with TECS, CBP vetting, and ATS. The web interface will be built from the ground up. The ESTA back-end services will be constructed using various commercial off-the-shelf products.

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

For each stage of the systems development lifecycle (SDLC), "collection – use and disclosure – processing – retention and destruction," key issues were assessed, and privacy risks were identified. Integrity, privacy, and security were analyzed as part of the decisions made for ESTA in accordance with CBP security and privacy policy from the inception of ESTA, as demonstrated by the transition through the SDLC, certification and accreditation, and investment management processes. Particular areas that were identified as needing to be addressed during the development included: use of accurate data, system access controls, and audit capabilities to ensure appropriate use of the system.

9.3 What design choices were made to enhance privacy?

User access controls were developed in order to ensure that only the minimum number of individuals with a need to know the information is provided access to the information. External users, such as applicants and third parties, will not have access to PII submitted to ESTA, and internal users will only have access after completing and conforming to CBP's security and privacy policies. Audit provisions in conjunction with policies and procedures were also put in place to

ensure that the system is properly used by CBP officers and other authorized users within DHS and other government agencies.

The system is designed to provide the following privacy protections:

- Equitable risk assessment:
  - ESTA provides equitable treatment for all individuals. Equitable risk assessment is provided because ESTA interfaces with the same databases for every applicant in seeking to identify matches.
  - ESTA applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. ESTA is consistent in its comparison of associated data with individuals and is used to support the overall CBP counterterrorism, law enforcement, and public security missions.
  - ESTA supports a national screening policy that is established at the CBP National Targeting Center. CBP policies regarding inspections and responding to potential terrorists and other criminals seeking entry into the United States are documented in various CBP Directives and individuals with access to the system are trained on the appropriate use of the information.
- CBP's existing components and secure encrypted network:
  - System construction purposely included the re-use of components that have been proven secure and privacy compliant.
  - ESTA security processes, procedures, and infrastructure provide protection of data, including data about individuals that are stored in ESTA.
  - Encryption and authentication are the technical tools used to protect all ESTA data, including data about individuals.
- Privacy Officer:
  - ESTA will have a Privacy Officer to oversee mandatory privacy training for system operators and appropriate safeguards for data handling.

Additionally, access to ESTA PII data is limited to CBP, DHS, and other counter-terrorism, law enforcement, and public security officers who have gone through extensive training on the appropriate use of the information and CBP screening policies. These officers are trained to review the ESTA data and any associated information to identify individuals that truly pose a risk to law enforcement.

Responsible Officials

Beverly Good, Director, Admissibility and Passenger Programs – ESTA, U.S. Customs and Border Protection, Department of Homeland Security

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Regulations & Rulings, Office of International Trade, U.S. Customs and Border Protection, Department of Homeland Security

Reviewing Official

Hugo Teufel III
Chief Privacy Officer, DHS
(703) 235-0780

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security