1) Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2) System Information

2a) Date PIA was completed: April 8, 2011

2b) Name of system: Smart Traveler Enrollment Program

2c) System acronym: STEP

2d) IT Asset Baseline (ITAB) number: 27

2e) System description (Briefly describe scope, purpose, and major functions):

The STEP is a service of the American Citizen Services (ACS) program. The ACS program consists of a suite of tools for tracking and managing information pertaining to American citizens abroad. STEP allows American citizens to provide foreign travel or residential information electronically over the Internet via appropriate secure connections to the appropriate embassies or consulates to facilitate the provision of consular services, including emergency aid, to overseas American citizens. The STEP application accepts information from American citizens through a secure Internet web site hosted by the Department of State, creates records within the registration service, and replicates the information to the ACS application at the appropriate embassies and consulates. Additionally, STEP automatically relays its data to the Consular Consolidated Database (CCD). Once the data is available on the CCD, consular officers and other consular personnel are able to access STEP data through the CCD Consular Application.

From the internet-based user's perspective, the functionality of the STEP web site is relatively simple. Users access the STEP web site and are provided with an overview of registration, and instructions on how to register. Individuals register in STEP by submitting a unique username and password to create a user account. Users planning overseas travel may then provide designated destination(s) and period(s) of travel. Users living overseas may provide their foreign address information. The information may be gathered using Form DS-4024 (which can be found on the FOIA website) and provided to the user's local post. User information is then transferred to ACS at the appropriate designated post(s). Users may return to the web site to change any of their information by providing their username and password to access the site, edit their data, and re-submit their form electronically.

Some additional functions that will be supported beyond the basic registration service include display and distribution of travel warnings and other important information to registrants, data retrieval and reporting functions for Consular personnel, and web site administration functions.

2f) Reason for performing PIA: PIA Data Call

☐ New system

Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

2g)Explanation of modification (if applicable):

2h)Date of previous PIA (if applicable): Feb 16 2010

3) Characterization of the Information

The system:

☐ Does NOT contain PII. If this is the case, you must only complete Section 13.

☒ Does contain PII. If this is the case, you must complete the entire template.

3a)What elements of PII are collected and maintained by the system? What are the sources of the information?

U.S. Citizens: U.S. citizens who voluntarily register with STEP are the primary individuals about whom information is collected by STEP. Other U.S. citizens' information is collected only to the extent it is voluntarily provided by a registrant who lists a U.S. citizen as an emergency contact.

Employee information is not collected; this information is provided during the authentication process

Non-U.S. Citizens: Some non-U.S. citizen data may be collected in the process of providing services. For example, non-citizen relative information, contact information or service provider information may be collected during the process of providing services to American citizens overseas.

To create an account with STEP, users must provide:

- Traveler first name
- Traveler last name
- Traveler DOB
- At least one form of contact information: physical address; telephone number or email address.

In addition, during the registration process, STEP prompts users to enter passport information and the name, address, telephone number and email address for one emergency contact. However, this information is not required to complete the registration process.

Once an account is created, users have the option of registering their overseas residency and/or travel plans. To do so, users must provide:

- Name of country visiting or of residence
- Date of arrival in that country

- Address or phone number where staying while in that country

STEP prompts users to enter the following additional information:

- Date of departure from the country
- Duration of stay
- Purpose of visit
- Travel companion information including:
  - Name
  - Date of birth
  - Gender
  - County of citizenship
  - Relationship to user
  - Passport information
  - Address, telephone number and email address

STEP does not collect any additional data from users through the use of persistent tracking technologies (e.g. persistent cookies).

3b)How is the information collected?

STEP collects information from persons who voluntarily provide it by accessing the Department of State's secure internet web site registration page available at https://travelregistration.state.gov/ibrs/ui/. Persons may register individually or through third-parties such as travel agents. Additionally, consular officers or other consular personnel may create new registration records on a traveler's behalf if the traveler does not have access to the internet or otherwise requests this service. The paper application (Form DS-4024) can be found at the Department of State's FOIA website as follows:

The Department of State FOIA website: http://www.state.gov/m/a/dir/forms/c21447.htm

The Smart Traveler Enrollment Program (Form DS-4024):
http://www.state.gov/documents/organization/83011.pdf

The web forms used to collect applicant data within STEP are OMB approved. Per Public Notice 6796 in 74 FR 206, 55277 (Oct. 27, 2009). See also Public Notice 6670 in 74 FR 115, 28752 (Jun. 17, 2009); Public Notice 5633 in 71 FR 232, 70446 (Dec. 4, 2006); Public Notice 4472 in 68 FR 174, 53212 (Sept. 9, 2003); Public Notice 4310 in 68 FR 51, 12732 (Mar. 17, 1993); Public Notice 5489 in 71 FR 154, 45891 (Aug. 10, 2006). STEP requires each new user to create an account login ID and password. This and all other information provided by users – personal biometric data, emergency contact, and trip itinerary information alike - becomes part of their profile. Users can access their accounts to modify profile information at any time. The information is automatically sent by STEP to the ACS section of the post with responsibility for the location(s) of the indicated travel. It is accessible to any CCD user such as consular officers and other consular personnel in other posts.

3c)Why is the information collected and maintained?

The Department of State created STEP to facilitate the provision of services to American citizens overseas by allowing American citizens to notify the Department of their travel plans electronically 24 hours a day, 7 days a week. The required information identified in Section 3a above is necessary to identify and locate persons entitled to receive assistance from the U.S. government. The requested information identified in Section 3a above is designed to help consular officers and other personnel at overseas posts to provide any needed service in a timely manner.

3d) How will the information be checked for accuracy?

3d1) How will data collected from sources, other than DOS records, be verified for accuracy?

STEP uses ASP.NET server validation. ASP.NET automatically will pass back form field elements (textbox, dropdown) through a form post-back. STEP uses custom/standard validation controls; their main purpose is to validate the form fields. If the field is invalid it will be marked so and checked during the form post-back.

3d2) How will data be checked for completeness?

STEP calls for a minimum number of required fields to be completed. Users are prevented from continuing the registration process unless the information gathered meets specified standards. Required fields within STEP are in Section 3a of this document.

3d3) Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Each users' personal data will remain in the STEP database indefinitely. Data from STEP will be archived only with a specific task request from the Government Task Manager (GTM). Registrations will remain in the file unless edited or deleted by the registrant.

3e) What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of STEP:

- 8 U.S.C. 1104 (Powers and duties of Secretary of State)
- 22 U.S.C. 2651a (Organization of Department of State)
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens)
- 22 U.S.C. 1731 (Protection to naturalized citizens abroad)
- 22 U.S.C. 3904 (Functions of service)
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)
- 22 U.S.C. 4197 (Following testamentary directions; assistance to testamentary appointee)

- 22 U.S.C. 4802b (Overseas evacuations)

3f) Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The personal data collected by STEP is limited to user names, contact information and locations of travel. It is the minimum necessary to carry out the function of STEP as identified in Section 3(c) above. The STEP security and privacy controls in place are adequate to safeguard customer privacy. STEP utilizes numerous management, operational and technical security controls to protect the data in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

Access to the data for STEP is controlled through the use of user accounts with login and password requirements, and the use of roles. (Details regarding user roles can be found in the STEP/CTF System Security Plan)

4) Uses of the Information

4a) Describe all uses of the information.

The data collected through STEP is used to contact American citizens in the event of an emergency and to disburse post newsletters, inclement weather and travel alerts, warden messages, and other information relevant to the American citizen community living or traveling abroad. The information can also be sorted by posts to manage their contact lists as described in Section 4(b) below.

4b) What types of methods are used to analyze the data? What new information may be produced?

No new data or previously unavailable personal data will be created through derived data or aggregation of data collected in STEP. However, records created within the STEP system are available on the Consular Consolidated Database (CCD). Once this data is aggregated in CCD, it serves as both a backup for each post's transaction activity, and it allows the Bureau of Consular Affairs (CA) the ability to apply advanced metrics against the data. Whenever a record is updated within STEP, the information is replicated into the CCD where it is maintained.

Consular users have the ability to generate predefined reports of the STEP travel data entered by the registrants based upon selected criteria. Reports are used to help consular Users manage the registration records in the STEP system, especially in the event of an emergency.

The following reports can be produced from data collected in STEP:

1. Registrant Contact List - The Registrant Contact List Report provides a complete list of registrants that fit the report criteria. The list of registrants will include contact information in the destination country, any emergency contact information (if any), and the privacy waiver selection for each registrant in the list.

2. Registrant Email List - The Registrant Email List provides registrant email addresses in a format ready to be inserted into an email message or exported to a spreadsheet.

3. Registrant Lookup - The Registrant Lookup Report provides a summary list of registrants from which the consular User can choose to view a detailed report.

4. Registrant Lookup for Multiple Posts - The Registrant Lookup for Multiple Posts report provides a summary list of travelers who have registered visits not only at the post selected, but who have also registered for visits to other posts. The consular user can choose to view a detailed report for each registrant.

5. Organization Report - The Organization Report provides a list of the registrants for a particular organization by post or country.

6. Marked for Deletion List - The Registrant Marked for Deletion Report provides a summary list of registrants that have been marked for deletion. The consular user can choose to view a detailed report for each registrant.

4c) If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Not Applicable

4d) Is the system a contractor used and owned system?

STEP is a government owned system. Contractors are allowed to access the system and perform administrative tasks on the system. All contractors and government employees must complete the same security awareness training courses before access is granted. Contractors and government employees are also bound by the same security rules and standard operating procedures.

4e) Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Policies/procedures governing the disclosure of American citizen information are specified in various sections of 7 FAM Consular Affairs. The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records. All PII collected is utilized for a specific purpose and is necessary to allow the system to properly perform its duties.

Consular user access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categorization of information and help define distribution restrictions for some reports.

The CA post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized uses by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU.

5) Retention

5a) How long is information retained?

Users' personal data will remain in STEP indefinitely. Users can not delete their account. STEP users can delete/modify their registered trips, address, phone and email information. Users' personal data will remain in STEP indefinitely. Data from the STEP system will be archived only with a specific task request from the GTM under direction from the Bureau of Consular Affairs Office of Citizen Services (CA/OCS). Paper applications are held for one year from the date of acceptance at post for enrollments longer than 6 months in duration. Paper application records for shorter visits can be destroyed after the enrollment is completed in the consular application.

5b) Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.

Virtually all STEP data is subject to a limited lifecycle which is determined by the records retention schedule and the availability of archive resources. There is no established schedule to purge archived data or auditing data within STEP the privacy risks are mitigated through the controlled access and rules of behavior that govern the users of STEP throughout the lifetime of the data. Accuracy of the data is dependent on the individual users registering through STEP. It is the responsibility of each registrant to correct information which was incorrectly entered into STEP and to update information which was accurate when entered but has since changed.

6) Internal Sharing and Disclosure

6a) With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Access to STEP data is restricted to the following:

Department of State OpenNet-based Users with access to all STEP data

- STEP Administrator
- Overseas Consular Users
- Overseas Citizen Services Domestic Users
- Administrative Users (Web/System/Database)

Public Users with access only to their own data or to the data of persons for whom they are authorized to act as agents

- Individual Users
- Organizational Users (e.g.,Travel Agents)

6b) How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The following controls are in place establishing criteria, procedures and responsibilities regarding access to STEP:

For STEP Administrative Users and CA/OCS Domestic Users a certifying authority is responsible for reviewing each account request and creating the user account. Database administrative accounts are reviewed and approved by the CA ISSO, system and web administrator accounts are authorized by the Government Project Manager. All levels of access granted to STEP users are based on the concepts of least privilege and separation of duties.

A detailed description of the criteria, procedures, controls and responsibilities regarding access is documented in the STEP System Security Plan (SSP).

Public users access STEP through a secure web site. All public users must create a login to register a trip with STEP. Public user accounts are password protected.

6c) Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The aforementioned personally identifiable information is shared solely within the Bureau of Consular Affairs (CA), among cleared employees with role-based access to the data and is done so via secure transmission methods. All levels of access granted to STEP users are based on the concepts of least privilege and separation of duties. As such, the privacy risk from internal sharing is negligible.

For STEP, data on registrations is accepted into ACS by post ACS users. This allows post users to determine if the data is valid before accepting it into ACS. Access to the data is determined by user roles.

7) External Sharing and Disclosure

7a) With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

No agencies external to the Bureau of Consular Affairs (CA) have access to the data in STEP. Occasionally, limited personal information is shared with third parties described in 7b for the purpose of properly responding to a crisis.

7b) How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Consular officers and other personnel may, from time to time and on an as-needed-basis, share information obtained from STEP with third parties where necessary to preserve the health and safety of American citizens as indicated in the Overseas Citizens Services System of Records Notice.

Such parties may include transportation carriers and wardens living within the consulate district affected by a crisis. Carriers are provided only the minimal personal information necessary to respond to the crisis. Information is generally supplied pursuant to a Memorandum of Understanding (MOU) governing the use of the information.

Wardens are provided only the minimal personal information necessary – usually name and contact information – to allow them to pass along information to the American citizen. Information is transmitted to wardens by hardcopy whenever possible, and must be returned by wardens upon completion of their tenure.

Each warden is required to sign a MOU governing the use and security of personal information provided by the Department of State.

7c) Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risk to privacy of sharing information obtained through STEP with participants of the warden system is that the information provided will be used for unauthorized purposes, lost, stolen or misappropriated.

These risks are mitigated by limiting the sharing of information with third-parties that have a need to know based on the Overseas Citizens Services System of Records Notice (STATE-05). The Department may require a third-party to sign a memorandum of understanding outlining the permitted uses of the shared information.

With respect to wardens, the use of wardens is authorized by 22 U.S.C. 4802(b) and 31 U.S.C. 1342. The warden system is an essential tool in the provision of consular services to American citizens overseas. Each warden is required to sign a memorandum of understanding governing the use and security of personal information provided by the Department of State. The Department of State subjects the warden system to periodic testing.

8) Notice

The system:

X Constitutes a system of records covered by the Privacy Act.

Provide the number and name of each applicable system of records

(visit www.state.gov/m/a/ips/c25533.htm for a list of all published systems):

- Overseas Citizens Services Records. STATE-05
- Overseas Records. STATE-25

☐ Does not constitute a system of records covered by the Privacy Act.

8a) Is notice provided to the individual prior to collection of their information?

The systems of records notice (SORNs) mentioned above cover the collection of information by STEP and provide notice to individuals of that collection. The web forms used to collect applicant data within STEP under this program are OMB approved and contain a Privacy Act statement. STEP requires the user to complete the Privacy Act notification; registrants are required to indicate that they have read the Privacy Act statement before registering a trip. The Privacy Act statement for STEP appears as follows:

8b) Do individuals have the opportunity and/or right to decline to provide information?

Privacy Act restrictions are strictly enforced by STEP and are automatically fully protected unless specifically waived by the American citizen.

American citizens have the right and opportunity to decline to provide the information, but services cannot be provided without their explicit acceptance of the terms.

8c) Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Yes. The Privacy Act screens for STEP allow American citizens to limit to whom their personal information may be shared.

8d) Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

STEP complies with all Privacy Act requirements for notice at the point of collection. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Therefore, this category of privacy risk is appropriately mitigated.

9) Notification and Redress

9a) What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

STEP users must create a user account and login to enter their information. Individuals may delete, amend, or supplement the information they provide at any time by logging into their online STEP account.

9b) Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Since STEP is Privacy Act-covered, formal procedures for notification and redress exist. Therefore, this category of privacy risk is appropriately mitigated. Individuals may delete, amend, or supplement the information they provide at any time by logging into their online STEP account.

10) Controls on Access

10a) What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

- All Consular users, including external agency users, are screened prior to their employment with the Department or their respective agency. The Bureau of Diplomatic Security (DS) is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before given access to the OpenNet and any CA/CST system, including STEP, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.
- It is mandatory for all Department of State employees and contractors to pass an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.
- Each domestic organization has at least one Bureau of Consular Affairs (CA)systems administrator who is responsible for managing the non-public users within the organization. CAsystems administrators are government employees who use STEP to approve account requests and assign STEP roles appropriate for each user's job requirement. STEP roles determine what a non-public user can do on STEP.
- The CA administrator determines the access level to CA applications controlled by Consular Shared Tables (CST) needed by a non-public user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Contractors who support STEP are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of STEP hardware and software must have a level "Secret" security clearance. Once the highest-level background investigation

required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing STEP.

STEP has assigned access authorizations that are enforced in accordance with 12 FAM 629.2-1 and 12 FAM 643.2-1. The following sections describe the level of access/privileges assigned to each STEP user group:

DoS OpenNet-based Users

STEP Administrator

The Administration (Admin) application of IRBS allows consular users to:

- Maintain Travel Information functionality
    - The Maintain Travel Information functionality of the Admin application allows travel.state.gov (TSG) users to maintain the travel warnings and public announcements issued by the Department of State to post for their travelers
- Maintain FAQs functionality
    - The Maintain FAQs functionality of the Consular Application allows users to modify the content of the homepage of the STEP website.
- Validating Posts functionality.
    - The Validating Posts functionality of the Admin application allows users to assign one post to validate another's data in STEP.

Overseas Consular Users

The STEP Consular Application allows consular users to manage their posts' data in order to assist American citizens traveling to their post.

From the Consular Application home page, consular users can:

- Validate registrants and organizations
- Reject registrants and organizations
- Reassign registrants and organizations to another post
- Register new travelers and organizations
- Add trips to existing registrations
- Run reports on post data
- Send post email

Overseas Citizen Services Domestic Users

The OCS domestic users are comprised of the Washington, DC-based CA/OCS staff. These users require access to STEP data for the purposes of oversight and reporting.

Public Users

Individual & Organizational Users (e.g., Travel Agents)

The STEP Internet site allows Public Users to:

- Sign up for Travel Warnings, Public Announcements, and Consular Information Sheets issued by the Department of State via email for a country of choice
- Register trips and residence abroad online

10b) What privacy orientation or training for the system is provided authorized users?

In addition to the measures described in Sections 3(f) and 4(e) above, all personnel accessing systems residing on the OpenNet or OpenNet Plus are required to attend the following two security awareness-raising presentations:

- Diplomatic Security's Security Briefing
- Consular Affairs' in-house Security Awareness presentation

Both presentations require signed acknowledgement of the rules of behavior and include segments covering appropriate system usage and formal statements on the Rules of Behavior regarding Department of State computer systems.

NIST 800-53 Rev2 AT-2

(i) Once a CA employee user has been provided OpenNet access, they are required to attend CA specific security awareness training. All CA users are required to take two types of security training:

- Information Security (INFOSEC) Briefing - New CA users are required to attend a site-specific security briefing within 30 days of joining the Bureau.
- OpenNet Plus Online Training. Users who have taken this online training with another Bureau within the last year do not need to take the training again until after their one-year anniversary date. All other users are required to take the training within 5 days of receiving a CA logon.

Failure to take either training course can result in revoking a user's access to the Bureau's Information Systems.

13 FAM 331 Cyber Security Awareness Training

(ii) If significant enough change occurs with the STEP, or CTF systems, security awareness training will be provided.

(iii) All CA users are required to take annual security awareness training for OpenNet. It is a government-wide requirement that all users of Federal information systems receive annual cyber security awareness training. This mandate is satisfied by the Department of State through user completion of the PS800 Cyber Security Awareness Course. Users link to https://fsicsapps.fsi.state.gov/csa/login.aspx
5 FAM 845 SECURITY AWARENESS, TRAINING, AND EDUCATION

Public users who access STEP via the travel.state.gov web site are presented with Privacy and Computer Fraud and Abuse Act Notices that describe their expected behavior while accessing the STEP web site. In addition since the public user's registration is used to make their presence and whereabouts known in the event of an emergency, it is expected that these users would not want to misuse their own data.

10c) Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Adequate controls to limit access and to regulate the behavior of authorized users are implemented in STEP. Therefore, this level of privacy risk is negligible. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to detect and deter unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.) As a result of these actions, the residual risk is low.

11) Technologies

11a) What technologies are used in the system that involves privacy risk?

The system uses standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. There are no technologies used which employ commonly identified vulnerabilities that might cause an elevation of overall privacy risks.

11b) Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

The system does not use any technologies that are known to contain vulnerabilities that might cause undue privacy risk.

12) Security

12a) What is the security certification and accreditation (C&A) status of the system?

The Department of State operates STEP in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) of 2002 provision for the triennial recertification of this system, its most recent date of authorization to operate was August, 2007.