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

(a) Date PIA was completed: January 11, 2011

(b) Name of system: Tracking Responses and Inquiries for Passports

(c) System acronym: TRIP

(d) IT Asset Baseline (ITAB) number: 2677

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

TRIP is a web-based application that is composed of commercial-off-the-shelf (COTS) software that has been modified to meet functional requirements. TRIP allows Consular Systems and Technology (CA/CST) to maintain records of passport applicants that call the National Passport Information Center (NPIC) to inquire about their passport application status. TRIP allows the Customer Service Representatives (CSRs) to review Travel Document Issuance System (TDIS) passport application records, including inquiries made by passport applicants regarding the status of their passport applications. The CSRs are able to see a case history and generate notes on each case. Emails can be generated for each TDIS Passport agency user that can access the knowledge base which contains referenced Department of State information.

TRIP is located at NPIC in Lansing, Michigan. A second host site for contingency and disaster recovery is located in Phoenix, Arizona.

TRIP interfaces with the Front End Processor (FEP) system. TRIP uses FEP to query the TDIS application database for information pertaining to an applicant.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable): 12/30/2009

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.

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

TRIP collects and maintains the following personally identifiable information (PII) elements when applicants contact the NPIC to inquire about their passport status: name, home phone number, address, date of birth (DOB), Social Security number (SSN), and credit card number. The Customer Service Representative (CSR) searches TDIS by passport application number, applicant's SSN or applicant last name and DOB to retrieve pertinent passport application status information. TRIP is designed so that neither SSNs nor credit card numbers are maintained beyond the length of a call.

In addition, TRIP interfaces with TDIS, and the CSRs can only read, but not modify, the applicant's personal data. All of an applicant's PII can only be read from the TDIS response. No edits can be made in TDIS by any NPIC personnel. None of the application information in TDIS is modifiable when accessed by a CSR. The information from TDIS that is accessible to the CSRs includes: name, home phone number, address, date of birth (DOB) and SSN.

TDIS collects and maintains records related to applications for U.S. passports. TDIS includes the following categories of records:

- Passport books and passport cards, applications for passport books and passport cards, and applications for additional visa pages, amendments, extensions, replacements, and/or renewals of passport books or cards; and
- Records of lost and stolen passports.

Sources of the information are U.S. citizens applying for passports, other Department of State computer systems, passport specialists, and fraud prevention managers. The categories of record subjects in TDIS are individuals who:

- Have applied for the issuance, amendment, extension, or renewal of U.S. passport books and passport cards;
- Were issued U.S. passport books or cards, or had passports amended, extended, renewed, limited, or denied;
- Have corresponded with the Bureau of Consular Affairs (CA) concerning various aspects of the issuance or denial of a specific applicant's U.S. passport books or cards; or
- Have applied for additional visa pages to a previously issued and currently valid passport.

The PII in TDIS that is referenced by TRIP is maintained by TDIS. CSRs access this information and verify it with the passport applicant before giving out any private information regarding their passport application.

b. How is the information collected?

The information in TRIP is collected by telephone when the applicant calls NPIC and speaks to a CSR or via a web form filled out by the applicant at the NPIC website.

The information in TDIS is collected on any of several forms: Form DS-11 is used for passport applications from first time applicants; Form DS-82 is for persons applying to replace a passport issued within the past 15 years, who were over the age of 16 when the passport was issued, and who also provide the old passport with the application form; and Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. Form DS-5504 may be used to replace an emergency passport with a fully valid one, to make a change to the applicant's identifying information (e.g., name change due to marriage or court order), or to correct a printing error in their passport. Form DS-4085 is used to add visa pages to a previously issued and currently valid passport.

The above forms may be completed by the applicant on published paper forms available at many U.S. government office locations or may be completed online using web forms at the Department of State's public web site. If web forms are used, the applicant must still print the form and submit it as a hard copy with supporting documents.

c. Why is the information collected and maintained?

The name, date of birth, phone number, address, and SSN of inquirers is requested to allow TRIP Customer Service Representatives (CSRs) to verify the identity of inquirers before responding to phone inquiries for passport application status from U.S. citizens (any mail inquiries go directly to Passport Agencies). Note that TRIP is designed so that SSNs are not maintained beyond the length of a call. The verification process is designed to prevent fraud and ensure the privacy of U.S. citizens who have applied for passports. CSRs query TDIS through the TRIP standard query language (SQL) server database to view passport applicants' application updates.

d. How will the information be checked for accuracy?

The information requested of inquirers is confirmed against the information on the passport or passport application contained in TDIS. Accuracy of the information contained in TDIS (such as a passport application or submission of citizenship evidence) is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

A CSR can enter the applicant's Social Security number (SSN), passport application number or the applicant's last name and date of birth to search the TDIS database. CSRs do not have direct access to TDIS but can access TDIS via a TRIP/TDIS interface. CSRs will provide application status information found in TDIS after verifying the accuracy of the information submitted in the application with each applicant. If the applicant cannot be located by the TRIP system search of the TDIS system and he or she has applied for a passport, then the applicant's new application record has not been created in the TDIS system. This will occur when the applicant seeks a status the same day or week that he or she applied for the passport.

If an applicant's passport information is not already in TDIS, then the CSR cannot see the passport application data or status and cannot provide a passport application status update to the passport applicant. If, however, the applicant's application appears in TDIS and any of the information is incorrect (when the CSR verifies it with the passport applicant) then the CSR will request the correct information from the passport applicant and will send a notification email to the adjudicating passport agency requesting an update to the applicant's information in TDIS. CSRs have no ability to directly update an applicant's information.

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

The following authorities provide for the administration of the program supported by TRIP:

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- Executive Order 11295 (August 5, 1966)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)

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

With the collection of passport data, TRIP has high data element sensitivity and high data subject distinguishability. The primary risk is misuse by Department employees and contractors. Misuse of PII could result in a delay in processing passport applications, approving applicants who are not eligible, and denying applicants who are eligible. Misuse may also result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

These factors are mitigated through a very specific context of use, in that TRIP uses passport information to verify inquirer identity and to search TDIS passport records, and through a statutorily mandated obligation to protect confidentiality.

Considering the large amount of PII collected by TRIP and TDIS (and subsequently accessed by TRIP), the security and privacy controls in place are adequate to safeguard applicant privacy. The collection of PII is the minimum amount necessary to fulfill the statutory purposes of the system. Any remaining privacy risks inherent in the sources or methods of collection are mitigated by appropriate privacy and security controls detailed throughout this privacy impact assessment.

Specifically, TRIP 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.

4. Uses of the Information

a. Describe all uses of the information.

The TRIP system allows CA/CST to keep records on every contact with applicants who call NPIC to inquire about their passport application status. TRIP allows CSRs to bring up TDIS inquiries on passport application records and view the information by searching by the applicant's passport application number, SSN or the applicant's last name and DOB. The CSR then confirms the identity of the inquirer by requesting the inquirer's PII indicated in Section 3(a) above to ensure that it matches the information in the record. Once the information is confirmed, the CSR may then share the information in the record with the inquirer. Each CSR is able to see a case history as well as generate emails to the passport agency on each applicant if needed. Emails can be generated for each of the 22 Passport Agencies, and TRIP also enables each CSR user to access the knowledge base, which contains Department of State travel information that is referenced using the applicant's passport application number, SSN or the applicant's last name and DOB. The applicant's SSN is not maintained in the TRIP database beyond the length of a call. The applicant's passport application number, SSN or the applicant's last name and DOB must be given to the CSR each time they call to inquire about their passport.

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

A CSR enters the applicant's information (the applicant's passport application number, SSN or the applicant's last name and DOB) into TRIP in order to search the TDIS database. The initial step is to query the TDIS system and use the search results to verify if the applicant is already in the TDIS system. If the applicant's passport information already exists in TDIS, then the existing record will be used to relay a passport status to the applicant online or via phone. Upon verification by CSR that the TDIS response pertains to the caller, TRIP transfers the applicant's information into the CSR's call record in a read-only process. The caller's SSN is not maintained in the TRIP database beyond the length of a call. The CSRs cannot create new information directly in TDIS (changes or clarification to full names; address, phone numbers, incorrect recording of SSN, DOB, etc.) but can request the changes be made by persons with access to TDIS by typing the call notes in an email from within TRIP (that automatically retrieves applicant information from within the system) that is sent to the adjudicating agency either requesting additional information or relaying new information.

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

TRIP does not use any commercial information. TRIP merely accesses information contained in the TDIS system database. TDIS, owned by the Department of State, is considered a Federal Agency database.

d. Are contractors involved in the uses of the PII?

TRIP is a Department of State system that is developed and maintained by Peckham, Inc. The system is hosted at NPIC in Lansing, Michigan with a disaster recovery site located in Phoenix, Arizona. Contractors are involved with the design, development, and maintenance of the system. Privacy Act information clauses have

been inserted into all statements of work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of classified and other such information prior to working on the task.

e. 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.

Contractors involved in the design, development and maintenance of TRIP are required to have a Moderate Risk Public Trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of TDIS hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo 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. Contractor-owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

The internal users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users 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.

In addition, there are technical system security controls in place as described in Section 3(f) above.

5. Retention

a. How long is information retained?

TRIP is designed to maintain the name, phone number, address and date of birth of people calling NPIC for 180 days. Other PII (SSN, credit card number, if applicable) is not maintained beyond the end of the call to NPIC.

b. 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. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of TRIP throughout the lifetime of the data. Accuracy of the data is dependent on the individuals providing self-identifying information. The information is only retained for the amount of time that is required to perform the system's purpose.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, as stated in

the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records (per A-13-002-05 which has a 180 day retention period), they are immediately retired or destroyed in accordance with published Department of State record schedules as approved by the National Archives and Records Administration (NARA).

6. Internal Sharing and Disclosure

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

TRIP is accessible only through the Department of State OpenNet which is the Department of State in-house access intranet. The CSRs use the Internet Explorer (IE) browser to access the TRIP web portal located in Lansing, Michigan and Phoenix, Arizona. The backend TRIP servers consist of Contact Center servers, IQ servers, Microsoft SQL Database servers and Response servers. The CSRs connect to the Contact Center servers and submit the type of inquiry from the passport applicant into the SQL database. The CSR can access the information from the Travel Document Issuance System (TDIS) at the passport agency through TRIP. TRIP can be accessed by CSRs/management at the Lansing and Phoenix sites for the purpose of rendering to the applicant a status and for providing updates of applicant information via emails to the appropriate passport agency.

Access to the TRIP application is restricted to cleared, authorized Department of State direct-hire or contractor personnel via OpenNet. The TRIP application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

The information obtained by TRIP CSRs is used for the purpose of retrieving TDIS records to respond to passport applicant inquiries regarding the status of their applications.

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

Information is shared between TRIP and TDIS by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures

Additional or correct information obtained by CSRs from the passport applicant that relates to the processing of the applicant's passport is shared by CSRs via email with the appropriate passport agency. The passport applicant shares their SSN with the CSR on a one time basis in order to obtain a passport status. The passport applicant must relay their SSN each time they call because TRIP does not retain the applicant's SSN beyond the length of the call. Emails can be created by CSRs and sent from within TRIP using the local Exchange server as an SMTP relay point. Copies of TRIP-generated email content are not retained in the SMTP server, only message header information. Mail inquiries are not received at NPIC so they do not have to be handled.

Mail inquiries go directly to the agencies. CSRs must be approved by management and through the appropriate clearance processes to be given access to TRIP. All CSRs must have the appropriate TRIP application user identification and password before they can access TRIP and interact with applicants.

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

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of personal information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure including but not limited to annual security training, separation of duties, least privilege, personnel screening, and auditing.

Access to information is controlled by application access controls. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department of State regulations.

TRIP has formal, documented procedures to facilitate the implementation of its audit and accountability processes. The application produces audit records that contain sufficient information to establish what events occurred, the sources of the events identified by type, location, or subject. System administrators regularly review and analyze the application audit records for indications of suspicious activity or suspected violations of security protocols.

7. External Sharing and Disclosure

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

TRIP information will not be shared with other agencies for programmatic purposes. Only authorized Department of State CSRs and authorized passport agency personnel have access to the data in the system.

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

External access to any non-Department entities is strictly prohibited.

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

None. TRIP data is not externally shared or disclosed. TRIP data is only communicated with the applicant whose personal information has first been verified.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

Passport Records – STATE-26

Overseas Citizens Services – STATE-05

☐ does NOT contain information covered by the Privacy Act.

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

Individuals are made aware of the uses of the information prior to collection. U.S. citizens who contact CSRs via the National Passport Information Center (NPIC) website to inquire about their passport application are informed of the purpose for which certain information is asked of them and how it will be utilized. The NPIC website is found at http://cas2K3ftp01/passport/npic/npic 896.html. The following information regarding PII is posted on this page:

Use of the Internet to access your passport application involves the electronic transmission of personal information. When you complete and submit the "Status of Application Request," you are consenting to electronic transmission of the information you have requested. Your consent is effective during the entire time you are communicating with the National Passport Information Center (NPIC).

Passport Services can only release this information to the passport applicant or to the parent or guardian of an applicant under age 18.

Callers are informed at the start of a phone call that collection of PII may be asked of them for purposes of verifying the caller's identity or obtaining passport status information.

E-mailers are called back by a CSR, who, at the start of the phone call, states that PII may be asked of them for purposes of verifying the caller's identity or obtaining passport status information.

Mail inquiries are not received at NPIC. Main inquiries go directly to agencies.

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

Yes - They are advised that they can decline to provide the information requested; however, in doing so, they cannot have their passport status tracked by TRIP.

c. 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?

No other special uses of the information are permitted. Users are advised on the use of the information being collected.

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

Notice is given to individuals as described in Section 8(a) above. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

U.S. citizens that call NPIC for a status of their passport applications are notified either by the automated voice prompt service or the CSR that the purpose of the information/data they are required to give is for locating an accurate status on their pending passport. The information provided in the system of records notice (SORN) regarding passport records fully explains how the information may be used by the Department and how it is protected.

CSRs that utilize and have access to TRIP are restricted to cleared, authorized Department of State direct hires or contractor personnel. TRIP enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

9. Notification and Redress

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

A CSR retrieves information about an applicant's passport status from a TDIS response, having searched by the applicant's passport application number, SSN or the applicant's name and DOB. Upon verification by CSR that the TDIS response pertains to the caller, TRIP transfers the applicant's information into the CSR's call record in a read-only process. The caller's SSN is not maintained in TRIP database beyond the length of a call. TRIP can only be accessed via OpenNet by cleared, authorized Department of State direct hire or contractor NPIC personnel. If a change is required to a passport application, the proper procedures are relayed to the individual by the CSR handling the inquiry.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. 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?

Access to the TRIP application is restricted to cleared, authorized Department of State direct-hire or contractor personnel via OpenNet. To access the system, users must be an authorized user of the Department of State's unclassified network. Access to T2 Flex requires a unique user account assigned by a supervisor. Each authorized user must sign a user access agreement before being given a user account. The user access

agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The TRIP application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. System administrators can access the TRIP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entities is strictly prohibited.

Personnel accessing TRIP information must be authorized by NPIC management. Authorized personnel require a user ID/password to access TRIP information. User access to TRIP information is based on roles. The regular users (CSRs) are allowed to create records and append new data to those records via an email from within the TRIP system that is sent to the TDIS adjudicating agency that relays new information on the passport applicant. The supervisors are allowed to review and make necessary corrections to the passport applicant record in TRIP. The supervisors will create another call record in TRIP, to reflect subsequent additional actions on a caller's behalf that were not captured in the original call record dealing with the same customer, should that be required. All TRIP users have knowledge of the Foreign Affairs Manual/Foreign Affairs Handbook (FAM/FAH) policies regarding privacy and are required to obtain annual Cyber Security Awareness Training.

Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.)

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

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internal users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

c. 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.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated.

Also as mentioned earlier, the system audit trails that are automatically generated are regularly reviewed and analyzed. As a result of these actions, the residual risk is low.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

TRIP is web-based application with approximately 300 XP Professional workstations and 10 Windows 2003 Servers. TRIP uses a customized Commercial off-the Shelf (COTS) Customer Relations Management (CRM) software product called Microsoft Dynamics designed and developed by Microsoft. It is customized to track Department of State passport applicant inquiries regarding the status of their passport application. These are all tested, proven technologies, and they pose no additional privacy risks.

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

Since TRIP does not use any technology known to elevate privacy risk, the current TRIP safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

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

The Department of State operates TRIP 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 36 month authorization to operate expires February 28, 2011.