



Privacy Impact Assessment (PIA)

**Passport Records Imaging Systems
Management (PRISM)**

Version 04.01.00

Last Updated: February 27, 2014

1. Contact Information

Department of State Privacy Coordinator

Sheryl Walter
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** February 27, 2014
- b. **Name of system:** Passport Records Imaging Systems Management
- c. **System acronym:** PRISM
- d. **IT Asset Baseline (ITAB) number:** # 896
- e. **System description (Briefly describe scope, purpose, and major functions):**

Passport Records Imaging System Management (PRISM) manages archived images of passport applications for a United States passport. Used on-site at passport agencies and by Records Services, PRISM is a digital imaging system that scans and stores information in an easily retrievable format. The primary purpose of PRISM is to scan passport applications quickly, efficiently, and reliably and store these records for immediate access from any authorized Department PC terminal.

PRISM was developed in order to scan and track the application images attached to each application for a U. S. passport. Scanning is done only after the application has been completely processed, meaning that the passport must already have undergone adjudication, book printing and customer delivery, or the application has been denied. Scanned images of applications are maintained in PRISM for 100 years. The image information is also moved to the passport records archival database, Passport Information Electronic Records System (PIERS). The records need to be retained for 100 years due to the retention requirements of the original paper records. The records are used to verify citizenship, support residency requirements, help establish citizenship claims of descendants and conduct genealogical research. The National Archivist is considering their value as historical documents which would affect any determination of permanent retention.

- 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): N/A

h. Date of previous PIA (if applicable): October 27, 2010

3. Characterization of the Information

The PRISM 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?

The sources of data are the paper forms provided by the individual applying for the U.S. passport. These forms include many elements of personal information. Passport applicant information maintained by PRISM is collected from the following forms submitted by the applicant:

- Form DS-11, used for new passport applicants, requires the following information:
 1. Name
 2. Date of birth
 3. Sex
 4. Place of birth
 5. Social Security number
 6. Email address
 7. Primary telephone number
 8. Mailing address
 9. Previous names used (up to two)
 10. Parents' names, date of birth, place of birth, sex, and whether parents are U.S. citizens
 11. Height
 12. Hair color
 13. Eye color
 14. Occupation
 15. Employer or school name
 16. Additional telephone numbers (up to two)
 17. Permanent address if different from mailing address
 18. Emergency contact name, address, telephone number, and relationship to applicant
 19. Date and duration of planned travel and countries visiting

20. Marital status, Current or most recent spouse's name, date of birth, place of birth, and citizenship, date of marriage, and widowed or divorced date
 21. Name used on previous passport book, book number, date of issue, and status
 22. Name used on previous passport card, card number, date of issue, and status
 23. Color photograph
- 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. Form DS-82 requires the following information:
 1. Name
 2. Date of Birth
 3. Sex
 4. Place of Birth
 5. Social Security number
 6. Email address
 7. Primary telephone number
 8. Mailing address
 9. Previous names used (up to two)
 10. Name used on previous passport book and card, book and card number, and dates of issue
 11. Reason for any name change if different on prior passport book or card and place and date of name change
 12. Height
 13. Hair color
 14. Eye color
 15. Occupation
 16. Employer or school name
 17. Additional telephone numbers (up to two)
 18. Permanent address if different than mailing address
 19. Emergency contact name, address, telephone number, and relationship to applicant
 20. Date and duration of planned travel and countries visiting
 21. Color photograph
 - Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form 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 the passport. Form DS-5504 requires the following information:
 1. Name
 2. Date of birth
 3. Sex
 4. Place of birth
 5. Social Security number
 6. Email address
 7. Telephone number

8. Mailing address
 9. Previous names used (up to two)
 10. Name used on previous passport book and card, book and card number, and dates of issue
 11. Height
 12. Hair color
 13. Eye color
 14. Occupation
 15. Employer
 16. Additional telephone numbers (up to two)
 17. Permanent address if different than mailing address
 18. Emergency contact name, address, telephone number, and relationship to applicant
 19. Date and duration of planned travel and countries visiting
 20. Color photograph
 21. Current name if changed from that used on previous passport
 22. Correct name, date of birth, sex, and/or place of birth if incorrectly printed on previous passport
 23. Whether previous passport was limited for a year or less
- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport. Form DS-4085 requires the following information:
 1. Name
 2. Date of birth
 3. Sex
 4. Place of birth
 5. Social Security number
 6. Email address
 7. Telephone number
 8. Mailing address
 9. Current passport number and issue date
 10. Permanent address if different than mailing address
 11. Additional telephone numbers (up to two)
 12. Occupation
 13. Employer or school
 14. Emergency contact name, address, telephone number, and relationship to applicant
 15. Date and duration of planned travel and countries visiting
 - Form DS-10 (birth affidavit) is used in conjunction with a Form DS-11 when an acceptable birth certificate cannot be obtained for a person born in the United States. Note that this form requests information about the applicant and the person making the affidavit (i.e., the affiant). Form DS-10 requires the following information from the affiant:
 1. Applicant's name
 2. Applicant's sex
 3. Applicant's date of birth
 4. Applicant's place of birth
 5. Applicant's home address

6. Number of years the affiant has known the applicant
 7. Affiant's relationship to the applicant or the basis of the affiant's knowledge regarding the applicant
 8. Statement of all the facts known by the affiant about the applicant's birth
 9. Affiant's name
 10. Affiant's Social Security number
 11. Affiant's address
 12. Affiant's identifying document submitted
- Form DS-60 (affidavit regarding change of name) is used in conjunction with a Form DS-11 when the name which is used by the applicant (1) is substantially different from that shown on the evidence of citizenship, or (2) has been adopted without formal court proceedings and was not acquired by marriage. Note that this form contains information about the applicant and the person making the affidavit. Form DS-60 requires the following information from an affiant:
 1. Current name of applicant
 2. Approximate date current name was assumed
 3. Number of years the affiant has known the applicant
 4. Former name of applicant
 5. Applicant's date of birth
 6. Applicant's place of birth
 7. Number of years the affiant has known the applicant by the current and former names
 8. Affiant's relationship to the applicant
 9. Statement / explanation of the variance in name
 10. Affiant's name
 11. Affiant's Social Security number
 12. Affiant's address
 13. Affiant's identifying document submitted
 - Form DS-64 is used in conjunction with a Form DS-11 when a previous valid or potentially valid U.S. passport cannot be presented. Form DS-64 requires the following information:
 1. Identifying Information
 - a. Name
 - b. Whether name has changed since previous passport issued
 - c. Sex
 - d. Date of birth
 - e. Place of birth
 - f. Social Security number
 - g. Current address
 - h. Home telephone number
 - i. Work telephone number
 - j. Email address
 2. Lost or Stolen U.S. Passport Book/Card Information
 - a. How the passport was lost or stolen
 - b. Where the passport was lost or stolen
 - c. Date the passport was lost or stolen

- d. Whether and how many times applicant has lost other passports or had them stolen
 - e. Whether submitting an application for a new passport
 - f. Number and issue date of lost or stolen passport book and/or card
- Form DS-71 is used in conjunction with a Form DS-11 only when the applicant for a passport is unable to establish his or her identity to the satisfaction of a person authorized to accept passport applications. Form DS-71 requires the following information from an identifying witness:
(Note: Witness information is only protected PII if Witness is an American Citizen or LPR.)
 1. Passport applicant name
 2. Witness' relationship to the applicant
 3. Length of time the witness has known the applicant
 4. Witness' name
 5. Witness' residential address
 6. Witness' place of birth
 7. Witness' date of birth
 8. Witness' telephone number
 9. Witness' Social Security number
 10. Whether the witness has been issued a U.S. passport
 11. Witness' passport number
 12. Place of issue of witness' passport (if known)
 13. Date of issue of witness' passport

The passport acceptance agent fills in the following information:

14. Applicant's name on first form of ID and document number
 15. Applicant first ID place and date of issue
 16. Applicant first ID expiration date
 17. Applicant's name on second form of ID and document number
 18. Applicant second ID place and date of issue
 19. Applicant second ID expiration date
 20. Witness' name on form of ID and document number
 21. Witness ID place and date of issue
 22. Witness ID expiration date
- Form DS-86 is used when the passport applicant does not receive the U.S. passport card and/or passport book for which he or she applied. Form DS-86 requires the following information:
 1. Name
 2. Date of birth
 3. Contact telephone numbers
 4. Mailing address
 5. Guardian's signature if applicable

The passport acceptance agent fills in the following information:

6. Tracking number of non-received passport/card
7. Previous passport book and/or card numbers and issue place and date

- Form DS-3053 is used in conjunction with a Form DS-11 if a non-applying parent or guardian consents to the issuance of a passport for his or her minor child who is younger than 16 years old. Form DS-3053 requires the following information:
 1. Minor's name
 2. Minor's date of birth
 3. Parent/guardian name and signature
 4. Parent/guardian address
 5. Parent/guardian telephone number
 6. Parent/guardian email address
 7. Name and signature of notary
 8. Location of notary
 9. Notary commission expiration date
 10. Form of ID of non-applying parent/guardian, document number, place and date of issue, and expiration date

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the U.S. Department of State's public web site, www.travel.state.gov. If web forms are used, the applicant must print the form and submit it as a hardcopy with supporting documents to the mailing address indicated on the form, in person at a domestic passport office, or at a United States embassy or consulate. The web forms are provided by other Bureau of Consular Affairs systems. PRISM only processes hardcopy forms.

b. How is the information collected?

Information is collected directly from the applicant using one or more of the above forms. The PRISM system operates in three stages: application handling/documentation preparation, scanning, and quality control/archiving. During the first stage, approximately 60 to 90 days after applications are completed or denied, they are scanned locally at the agency. Alternatively, they are boxed and shipped to the Records Management Branch of the Information Management Liaison Division in the Bureau of Consular Affairs' Passport Services Directorate CA/PPT/S/TO/RS. The boxes are received by the CA/PPT/IML/R staff, and then queued for scanning and archival by PRISM. The scanning stage includes the unbinding of documents, clearing any folds within the forms, and removing any miscellaneous debris from the package. Forms are then scanned into PRISM using high-speed Imaging Business Machines, LLC (IBML) scanners. The scans capture a full image of the top of the application, which includes the application data and photograph. The IBML scanner collates the pages to ensure that all passport application records are kept in the same order in which they were received. Finally, in the quality control/archival stage all scanned images are reviewed through a comprehensive quality control process. Scanned images are examined for color, data accuracy, and readability. If a scanned image fails the quality check, the documents are re-scanned. Once the quality control check is passed, the original physical forms are re-boxed and sent to archival storage.

c. Why is the information collected and maintained?

Passport applications are scanned and maintained by PRISM for the purpose of archiving completed passport applications as required by law.

PRISM is used to scan passport applications quickly, efficiently, and reliably and to store these records for immediate access from any authorized PC terminal. PRISM is also used to populate PIERS (Passport Information Electronic Records System). PIERS is then used to provide authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data for the purpose of adjudicating passport applications, and confirming citizenship and eligibility of persons to receive other consular services.

d. How will the information be checked for accuracy?

Accuracy of the information on a passport application and 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.

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

8 U.S.C. 1104, Powers and Duties of Secretary of State

8 U.S.C. 1101-1503, Immigration and Nationality Act of 1952, as amended

22 USC Sec. 211a-218, 2651a, 2705 (2007), Authority of the Secretary of State in granting and issuing U.S. passports

8 U.S.C. 1185, Travel Control of Citizens

26 USC 6039E, Information Concerning Resident Status

Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001

Executive Order 11295; 31 FR 10603 Rules Governing the Granting, Issuing, and Verifying of United States Passports, August 5, 1966

22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports and Visas

8 U.S.C. 1401-1503 (2007), Acquisition and Loss of U.S. Citizenship or U.S. Nationality use of U.S. Passports

8 U.S.C. 911, 1001, 1541-1546 (2007), Crimes and Criminal Procedure

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, PRISM has high data element sensitivity and high data subject distinguishability. The primary privacy risk is:

- Insider threat – employee misuse of data.

The consequences to organizations or individuals who PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation

- Blackmail
- Identity theft or assumption
- Account takeover
- Unauthorized release of sensitive information
- Threats to personal safety, discrimination, or physical harm
- Harm to Department of State programs or the public interest
- Administrative burdens, civil liability, financial loss, and loss of public reputation and public confidence for the Department of State

Numerous management, operational, and technical security controls are in place 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). PRISM application data is protected by multi-level system security. The multi-level system security includes OpenNet security, PRISM application security, Department of State site physical security and management security. These controls include regular security assessments, physical and environmental protection, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewall, intrusion detection systems, and antivirus software), training, and audit reports. In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application.

PRISM collects the minimum amount of personally identifiable information (PII) required to satisfy the statutory purposes of the system, as well as the mission of the CA Bureau as identified in Section 3c above. Access, authorizations, and permissions are granted at a level commensurate with the user's "need-to-know" as part of their official job duties and database management.

4. Uses of the Information

a. Describe all uses of the information.

Authorized Department of State employees use the system to have quick, efficient, and reliable computer access to the scanned images of passport applications throughout the passport issuance process for the purpose of adjudicating passport applications and confirming citizenship and eligibility of persons to receive other consular services. PRISM data also serves an archival purpose as part of PIERS.

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

PRISM performs no analysis of the scanned application images or produce any new information. However, the scanned images are used for analysis performed in other Consular Affairs systems such as facial recognition in the Travel Document Issuance System (TDIS).

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

No commercial information, publicly available information, or information from other Federal agency databases is used in PRISM. All of the information in PRISM is derived from completed U.S. passport applications.

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

PRISM is a government owned system that utilizes government off the shelf software (GOTS) and is developed, maintained and supported by contractors. All users were required to pass annual computer security and privacy awareness training, and to sign non-disclosure and rules of behavior agreements.

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.

PRISM is a government system. It is supported by contract employees, who support U.S. government employees in their maintenance of the system.

Contractors who support PRISM are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain U.S. Government agencies (e.g., criminal law enforcement and Department of Homeland Security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. Contractors involved in the development or maintenance of PRISM 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.

5. Retention

a. How long is information retained?

The established retention period for electronic records in PRISM is presently 100 years in accordance with published record schedules as approved by the National Archives and Records Administration (NARA). The disposition schedule for U.S. citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

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 that inaccuracies will develop as a consequence of aging.

Regular backups are performed and recovery procedures are in place for PRISM. When records have reached the end of their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration's disposition schedules.

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?

Information is only shared within the Bureau of Consular Affairs. PRISM is used to populate PIERS (Passport Information Electronic Records System), which is used to provide authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data for the purpose of adjudicating passport applications, and for confirming citizenship and eligibility of persons to receive other consular services.

To support passport application processing, the Bureau of Consular Affairs oversees a network of facilities that may internally share or disclose the personal information collected and maintained in PRISM to personnel with a "need-to-know". These facilities include approximately two dozen regional passport agencies, a special issuance agency, three national processing facilities, the National Passport Information Center, and the Headquarters offices in Washington, DC. The information may also be shared in a law enforcement inquiry, and/or in an emergency situation subject to the provisions of the Privacy Act.

The information shared is the information listed on the application regarding the individual and adjudication notes made by the passport examiner. PRISM redacts the name of the reviewing official.

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

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Controls built into the OpenNet GSS, including routers and Network Intrusion Detection Systems (NIDS), provide network level controls that limit the risk of unauthorized access from all IP segments. CA systems that interface with PRISM are strictly controlled by routers and NIDS rules sets that limit ingress and egress to PRISM.

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.

Vulnerabilities and risks are also mitigated through the system authorization process. NIST recommendations are followed to ensure that appropriate security controls are applied for all PII data in transit and in storage.

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?

PRISM does not interface with external entities. Persons or government agencies external to the Department of State's intranet are not able to connect to PRISM.

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

PRISM does not interface with external entities. Persons or government agencies external to the Department of State's intranet are not able to connect to PRISM.

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

PRISM does not interface with external entities. Persons or government agencies external to the Department of State's Intranet are not able to connect to PRISM.

8. Notice

The system:

<input checked="" type="checkbox"/>	Contains information covered by the Privacy Act. Provide number and name of each applicable system of records. Passport Records – STATE-26
<input type="checkbox"/>	Does NOT contain information covered by the Privacy Act.

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

Yes. Individuals are made aware of the uses of the information on the forms used to collect it identified in Section 3(a) above. Each published form associated with PRISM contains a Privacy Act statement in conformance with the requirements of the Act. Each form (including online web forms) exhibits an OMB authorization number indicating it is an approved information collection. The website that provides applicants the ability to complete an electronic application contains a tailored website privacy policy that describes the terms of use of the personal information provided.

Notice is also published in the System of Records Notice (SORN) titled STATE-26, Passport Systems. By providing the information requested at the initial request for passport or passport renewal, processing and issuance of the passport, U.S. citizens are consenting to the use of the information for its identified purpose.

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

An application for a passport is a voluntary action by a record subject. With the exception of his or her Social Security Number, an applicant is not legally required to provide the information requested on the passport application form. However, failure to do so may result in either Passport Services' refusal to accept the application or in the denial of passport services.

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. No other special uses of the information are permitted. Users are advised on the use of the information being collected. This process has occurred during the first-time passport request or passport renewal request, payment and issuance.

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 notice offered is reasonable and adequate in relation to the system's purposes and uses. The risks associated with individuals being unaware of the collection are mitigated through restricting access to PRISM to cleared, authorized Department of State employees and contractor personnel. PRISM 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?

PRISM contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in section 8 above, and in rules published at 22 CFR 171. The procedures inform individuals about how to inquire about the existence of records about themselves, how to request access to their records, and how to request amendment of their records. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of passport records on grounds pertaining to law enforcement. These exemptions are in the interest of national defense and foreign policy, if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. They are published as agency rules at 22 CFR 171.

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 system is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access

agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes the 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 the logon.

The level of access for the user restricts the data that may be seen and the degree to which data may be modified. Non-production uses (e.g., testing, training) of production data are limited by administrative controls. Activity by authorized users is monitored, logged, and audited.

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

All users are required to undergo computer security and privacy awareness training prior to accessing the system and must complete refresher training yearly in order to retain access.

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 restrict access to only system administrators and are regularly reviewed. 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 judged to be acceptable.

11. Technologies

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

PRISM operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other external business applications or technologies. No technologies that are known to elevate privacy risk are employed in PRISM.

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

Since PRISM does not use any technology known to elevate privacy risk, no additional security controls are needed.

12. Security

a. What is the security assessment and accreditation (A&A) status of the system?

The Department of State operates PRISM 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 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, the triennial assessment and authorization of this system is underway and is expected to be completed by March 2014. This document was updated as part of that process.