MRTD PKI and SDS

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Machine Readable Travel Document (MRTD) Public Key Infrastructure (PKI) and Signature Delivery Service (SDS)

(b) Bureau: Information Resource Management (IRM/FO/ITI/SI)

(c) System acronym: MRTD PKI & SDS

(d) iMatrix Asset ID Number: 893

(e) Reason for performing PIA: Upcoming system Assessment & Authorization (A&A)

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒ Yes
☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The authorization to operate (ATO) is expired as of March 2016. The system was scheduled to perform reauthorization before the 2016 expiration date. After the assessment started, it was identified by IRM/IA and confirmed by System Owner personnel that major system changes were in progress. IRM/IA and System Owner personnel agreed to hold off on the reauthorization until the changes were completed. At that time, there was no recommendation to request an ATO extension. By the time system changes were completed, System Owner personnel assigned to the assessment had left the Department with no replacement to carry on the ATO task. In addition, the AODR assigned to the system changed. After the System Owner personnel was replaced, efforts to update the MRTD PKI & SDS security documentation for the reauthorization began. At the end of 2018, IRM/IA and the System Owner began to coordinate a schedule to reauthorize the system. During this current assessment the Security Control Assessor

(SCA) left the Department 1/3/2020 and a new one has been assigned. Due to this, the anticipated completion date is March 2020.

(c) Describe the purpose of the system:

The MRTD PKI & SDS is a system that enables digital signing of data embedded in the Consular Affairs issued US electronic passports. The PKI component issues the certificates used by the SDS component to digitally sign the passport data and create a digital signature hash. The MRTD PKI & SDS uses cryptographic solutions to digitally sign the e-passports. This provides border entry and exit points around the world the ability to validate that the US passport presented has been issued by an authorized US authority (i.e. DOS).

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

MRTD PKI uses the following Passport information, provided by Consular Affairs Front End Processor system, to digitally sign the Passport: type of document, issuing state, surname/given name, document number, nationality, date of birth, sex, date of expiry, application number, place of birth, chip number, date of issue, and authority.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

This Certificate Policy (CP) was established under the authority of and with the approval of the Federal CIO Council. Under 44 U.S.C. § 3603, the CIO Council is authorized to develop and improve agency practices for the use and operation of Federal Government information resources. The Federal Information Security and Modernization Act, P.L. 113-283, requires agencies to comply with such policies, procedures, standards, and guidelines. 44 U.S.C. § 3554(a)(1)(B).

The Department implements the CP through a Memorandum of Agreement between the Federal PKI Policy Authority and the Department of State dated August 15, 2018.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☐ Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

☒ No, explain how the information is retrieved without a personal identifier.

The PKI component issues the certificates used by the SDS component to digitally sign the passport data and create a digital signature hash. Certificate information, in the PKI component, is searchable by certificate attributes (i.e. certificate issue date, certificate serial number, or certificate subject name). The SDS component does not have any information stored within it, therefore information searching is not applicable.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒ Yes ☐ No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): N1-GRS-07-3.
- Length of time the information is retained in the system: Information retained for the life of certificate, which is 15 years, in the system.
- Type of information retained in the system: Certificate information: certificate issue date, certificate serial number, certificate subject name.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐ Yes ☒ No

- If yes, under what authorization?

(c) How is the information collected?
The information used by the MRTD PKI & SDS is provided by DOS Consular Affairs Front End Processor (FEP) information system.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?
DOS Consular Affairs is responsible for the accuracy of the information provided to the MRTD PKI & SDS information system. MRTD PKI & SDS uses this information to digitally sign the passport.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
DOS Consular Affairs is responsible for making sure the data used by MRTD PKI & SDS is current.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not use information from commercial sources nor is the information publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, this is the responsibility of the DOS Passport office.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Individuals grant consent through the underlying U.S. Passport application process managed by the DOS Passport office.
- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Privacy concerns influenced the determination of the amount of information needed for MRTD PKI & SDS to fulfill its purpose of digitally signing the information provided by the Consular Affairs Front End Processor (FEP) information system. Only the PII required to carry out this function is collected. This is to avoid the MRTD PKI & SDS not having the proper security controls in place to secure the information collected.

5. Use of information

(a) What is/are the intended use(s) for the information?
The intended use(s) for the information are to support DOS passport issuance by digitally signing the information included on the passports.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internal Sharing: The MRTD PKI & SDS signature response (i.e. DOS digital signature), which contains the hashed PII from the DOS Consular Affairs Front End Processor (FEP), is shared internally with the DOS Consular Affairs Front End Processor (FEP) information system only.

There is no external sharing of PII from MRTD PKI & SDS.

(b) What information will be shared?

The information shared with DOS Consular Affairs Front End Processor (FEP) is: type of document, issuing state, surname/given name, document number, nationality, date of birth, sex, date of expiry, application number, place of birth, chip number, date of issue, and authority.

(c) What is the purpose for sharing the information?

The purpose of the system sharing the digitally signed items documented in the DOS issued passport is to provide DOS Consular Affairs the ability to verify whether a DOS issued passport is authorized or not.

(d) The information to be shared is transmitted or disclosed by what methods?

The information to be shared is transmitted by using the Transport Layer Security (TLS) protocol to establish a secure connection between the MRTD PKI & SDS system and the Front End Processor (FEP) system.

(e) What safeguards are in place for each internal or external sharing arrangement?

In addition to the information transmission method mentioned above, safeguards that are in place for the internal sharing arrangement is that access to the information being shared is limited to authorized Consular Affairs and IRM/FO/ITI/SI personnel assigned to the supporting systems. In addition, the information shared is limited to an amount which is required to meet mission essential activities.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns that were identified regarding sharing information from MRTD PKI & SDS with CA's FEP information system is ensuring the confidentiality and integrity of the digital signature. The confidentiality concern was addressed by ensuring that only authorized personnel assigned an IRM/FO/ITI/SI/IIB/PKI Program Office Trusted Role, with a need-to-know, are allowed access to the MRTD PKI & SDS information system. The integrity concern was addressed by implementing a technical solution which verifies that the MRTD PKI certificate used to digitally sign the passport is valid and meets the MRTD PKI certificate policy.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals do not have access to their information in the MRTD PKI & SDS system. Information is stored in DOS Consular Affairs Front End Processor (FEP) information system.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

DOS Passport office is responsible for these procedures as information is not stored in the MRTD PKI & SDS information system.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

DOS Passport office (Consular Affairs bureau) is responsible for notifying individuals of these procedures. Consular Affairs provides the procedures on the following site https://travel.state.gov/content/travel/en/passports/apply-renew-passport/change-correct.html. To begin the process, individuals are required to submit the DS-5504, Application for U.S. Passport (Corrections, Name Change Within 1 Year of Passport Issuance, and Limited Passport Holders), to the Passport office.

8. Security Controls

(a) How is the information in the system secured?

The information used or stored in the MRTD PKI & SDS information system has logical (i.e. Role Based Access Control implemented, firewalls) and physical access restrictions (i.e. use of DOS Diplomatic Security armed guards securing facility system resides in, badge readers, CCTV) limited to IRM/FO/ITI/SI/IIB/PKI Program Office personnel assigned a PKI Trusted Role.

All MRTD PKI & SDS information system components reside in DOS ESOC datacenters which require authorization for access to the datacenters. In addition, system components (i.e. servers) are physically secured in a “Strong Room” within the datacenters which has a combination door that requires two combinations held by PKI Trusted Role personnel to be opened (i.e. Two-Person Control). This process is leveraged to support efforts for logical access to the information system.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Only IRM/FO/ITI/SI/IIB/PKI Program Office personnel assigned a PKI Trusted Role are authorized to access the MRTD PKI & SDS information system for official work. Personnel receive this approval by senior management within the IRM/FO/ITI/Systems Integrity (SI) division.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Logically there are logs collected to determine when authorized individuals access the information system's components. Physically, there are badge readers at all datacenter locations used for access to the datacenters the information system resides in. In addition, sign-in/out logs required to be completed when entering and exiting the "Strong Room" which the system components are located. DOS ESOC datacenter personnel are responsible for monitoring, recording, and auditing personnel that have access or are authorized for escort within the DOS datacenters. IRM/FO/ITI/SI/IIB/PKI Program Office has an internal PKI auditor which reviews system component audit logs and sign-in/out logs.

(d) Explain the privacy training provided to authorize users of the system.

All users of the system are responsible for the issuance and management of PKI certificates. All are provided the PS800 Cyber Security Awareness course, which has a privacy module, during their initial employment date and annually, which addresses the protection of government-owned information. All foreign service, civil service and locally employed staff that handle PII are required to take the mandatory FSI course, PA 459, Protecting Personally Identifiable information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

The database in which the certificates and digital signature hashes reside is encrypted. In addition, only authorized personnel can access the MRTD PKI & SDS system and manage, e.g., update and patch, the MRTD PKI & SDS application. Physical access to the system requires access to the facilities housing the systems, which can only be accessed under two-person control (as explained in 8(b)).

(f) How were the security measures above influenced by the type of information collected?

The security measures above were influenced by the type of information collected to guarantee that the appropriate and applicable protections ensure the information provided to the MRTD PKI & SDS information system would not be compromised by unauthorized access or exposure. The security measures mentioned in 8(e) ensure the confidentiality of the information will not be compromised by limiting the access to the system, logically and physically, to authorized PKI Program Office personnel assigned to the MRTD PKI & SDS information system. The security measures mentioned in 8(e) also ensure the integrity of the information will not be compromised by implementing hashing and encryption technologies that are used to validate that the data within the system has not been tampered with.

9. Data Access

(a) Who has access to data in the system?

Though the system does not store the PII it uses to produce certificates and digital signatures, only authorized IRM/FO/ITI/SI/IIB/PKI Program Office system engineers and administrators have access to the system. Authorized personnel is defined as personnel that have been assigned a PKI Trusted Role by the IRM/FO/ITI/Systems Integrity (SI) division senior management.

(b) How is access to data in the system determined?

Access to data in the system is determined by the roles and responsibilities for an individual in the IRM/FO/ITI/SI/IIB PKI Program Office. Once a role is determined, a request is made by the IRM/FO/ITI/SI Service Lead to the PKI Program Manager to approve assigning the individual a PKI Trusted Role. After approval, the PKI Trusted Role individual is provided access to the information system based on their role.

When a role/personnel change occurs that requires removal of the individual’s account, a request is made by the IRM/FO/ITI/SI Service Lead to the PKI Program Manager to approve removal of the individual from having a PKI Trusted Role. After approval, the system’s role appointment memo is updated and signed by the PKI Program Manager and the individual’s system account(s) is disabled. Disabling instead of deleting of the account occurs to protect the integrity of audit logs containing activities by the account assigned to the individual. In additional, physical access to the rooms housing the system are removed and any door and safe combinations assigned to the individual are changed.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Only authorized staff of the PKI Program Office that have been assigned a PKI Trusted role are assigned access to the MRTD PKI & SDS information system. These users have access to all data in the system.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

There are physical controls in place to prevent the misuse of data by users having access to the data. Two-person access control is in place to access this data as well as the requirement to have authorized approval to physically access the ESOC datacenter facilities which the MRTD PKI & SDS system resides in. In addition, there are entrance/exit logs to document when access to the facilities housing the MRTD PKI &

SDS system occurs. These logs are reviewed by the PKI Program Office internal auditor. All personnel having access to the system as PKI Trusted Roles have been vetted thoroughly by the U.S. Office of Personnel Management (OPM) presenting them with a Top Secret (TS) clearance or an interim TS.