PRIVACY IMPACT ASSESSMENT

Enterprise Payment Service (EPS)

1. Contact Information

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

2. System Information

(a) **Name of system:** Enterprise Payment Service

(b) **Bureau:** Consular Affairs (CA)

(c) **System acronym**: EPS

(d) **iMatrix Asset ID Number:** 260640

(e) **Reason for performing PIA**:

☐ 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 Enterprise Payment Service Authorization-To-Operate expiration date is June 30, 2020.

(c) Describe the purpose of the system:

The Enterprise Payment Service (EPS) is a building block of the Consular Shared Tables (CST) Enterprise Architecture that provides a reusable payment collection capability to CST applications that need to collect fees for services from their consumers. The service uses pay.gov's Trusted Collection Service (TCS) as the underlying payment service provider. The pay.gov web-based application is owned and operated by the Department of Treasury. EPS allows U.S. citizens and non-U.S. citizensto pay for passports, visas, and other services offered by the Bureau of Consular Affairs. EPS interfaces with CST service applications that require fees for services.

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

- Payment Account Name (First, Last and Middle Initial)
- Payment Account Holder Personal Address
- Email Address
- Full credit card/banking account information is transmitted for payment via Pay.gov. However, account information stored within EPS contains only a masked account number (last 4 digits of account number) to support settlement inquiries

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

- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C. §§ 211a-218, 2705 Passports and Consular Reports of Birth Abroad (CRBAs)
- 22 U.S.C. § 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 U.S.C. § 3927 (Chief of Mission)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 22 CFR Part 22Schedule of Fees for Consular Services and authorities cited therein; see 83 FR 4425-4428, January 31, 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):

STATE-05 Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
STATE-39 Visa Records, June 15, 2018
STATE-26 Passport Records, March 24, 2015

Note: The EPS Web Service, a function within EPS, will permit the search of a previously submitted payment transaction based upon a person or organization's billing information (name, address, bank account number(last four numbers) etc.).

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

(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 .)

Schedule number Department of State Records Disposition Schedule:

A-13-001-5a & b: Passport Accounting Records – Accounting records showing money received, deposited, or refunded by Passport Services. Also includes copies of cash receipts.
Description: Consular cash receipts (DS233)
Disposition: Destroy when 5 years old.
DespAuthNo: N1-059-04-02, item 5a & 5b.

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 (are U.S. citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security numbers (SSNs), is the collection necessary?
☐Yes ☒No (SSNs are not collected)

- If yes, under what authorization?

(c) How is the information collected?

U.S. citizen:
Individuals seeking to renew their passport or to obtain other services online would go to the Travel.State.Gov public facing website to access the link to request a specific service or complete a hard copy of the Department of State form for the in person requested service. For online requests, at the point where payment for the service is required, EPS directs the individual to pay.gov where PII is entered and payments are made. Once the payment is made, a tansaction completion notice is directed back to EPS where only the last 4 digits of account numbers are maintained in the EPS system and an electronic receipt is created.

For in person service requests, the information is collected directly from the applicant in person who is requesting a fee-based consular service. This information is either manually entered or automatically collected when the credit card is swiped.

(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?

It is up to the individual entering the information to ensure accuracy. Pay.gov checks the accuracy of payment information such as card number. If there are discrepancies with the card number the transaction will be denied.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Data remains current by virtue of data checks with other DoS CA/CST systems and applicant input into the system where the application is entered (i.e., Consular Electronic Application Center (CEAC) Automated Cash Register System (ACRS), and Electronic Consular Report of Birth Abroad application (eCRBA) which is a component of the Consular Consolidated Database (CCD)). Mismatched data checks are resolved before an application moves forward for payment.

(g) Does the system use information from commercial sources? Is the information publicly available?

No. EPS does not use commercial or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

EPS does not collect data directly from applicants. Rather, the information stored in this system comes from CA/CST systems processing applicant requested services e.g., passport services for payment. Notice about the collection of data is provided to the individual by the system where the application is entered requesting the specific service.

(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?

-If no, why are individuals not allowed to provide consent?

EPS is not a customer-facing application and therefore will not interface directly with customers paying for consular services. EPS is a service accessed by other systems. The consent is provided at the point of collection for those systems which process the requested services: CEAC, ACRS, and CCD-eCRBA system.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items listed in Question 3d are the minimum necessary to perform the financial transactions required by this system. Concerns included unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. Impact is minimized, as collection of PII is limited to only what is required for the system to perform the function for which it was intended to process payments for services rendered.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the information is to facilitate financial transactions for consular services by providing a simplified payment method.

(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. The PII is used according to the stated purpose for which the system is designed: to process payments. Payments cannot be completed without the minimal PII collected by this system.

(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?
N/A

(2) **Does the analysis result in new information?**
☐Yes ☒No

(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.

The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique

processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the EPS system will be shared internally with other CA systems ACRS, CEAC, and CDD-eCRBA as mentioned previously.

Externally, information will be shared with the Department of Treasury (via pay.gov) for the purpose of processing a payment for consular services.

(b) What information will be shared?

Name, address, and credit card number (only the last 4 digits will be saved) will be shared with internal and external organizations.

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

The information is shared in order to process payments for Consular Affairs services.

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

All exchanges between CA system applications and EPS, and between EPS and Department of Treasury (i.e.,pay.gov), are transmitted electronically (database to database) via secured transport layer security methods approved by the Department of State policy for handling and transmission of sensitive but unclassified information.

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

Internal:

EPS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to assist with its data transport across the network with internal CA systems listed in paragraph 4.i. The TCP/IP protocol suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking and header checks. The server to server connection between all the system servers is protected using Secure Socket Layer with encryption.

External:

The information transmitted to pay.gov is secured using transport security as well as encryption. An interagency agreement is in place with the Treasury Department outlining safeguards in accessing and the transmission of data with the DoS.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles or authorization, and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.
b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

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

Applicants do not have access to their information directly on the EPS system; however, procedures for access and redress are published in the Privacy Act System of Records Notice (SORN) STATE-05 Overseas Citizens Services Records and Other Overseas Records; STATE-26 Passport Records and STATE-39 Visa Records, depending on the service application request associated with the fee. In addition, procedures are published on the Department of State public website.

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

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.
Individuals cannot correct information directly in EPS. EPS accepts transactions from other CA systems (ACRS, CEAC, and CCD-eCRBA). Applicants can change information via the original system where the service is being requested.

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

Information cannot be corrected in EPS. Individuals wishing to correct information can do so via the original system where the service was requested. In addition, procedures are published on the Department of State Privacy public website on how to correct information.

8. Security Controls

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

The EPS system is secured through the use of defense in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

EPS data is protected via authorized access controls for system and database administrators as defined by the Application Development Group policies. System Security Officer (SSO) and Integrated Services (IS) restrict access to information backup tapes to the system administrators. The organization employs multiple layers of automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Access to applications is controlled at the application level; there are additional access controls at the database level. All accounts for the system must be approved by the user's supervisor and the Information System Security Officer. The audit vault system is used to monitor all privileged access to the system in which audit logs are viewed at the application, database, and system level for abnormal activities. Users are uniquely identified and authenticated while logged in and activity can be traced to the person performing specific activities. Any violations are reported to senior management daily, if applicable. Data shared with the Department of Treasury is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by the Authorizing Officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) standards, including NIST 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(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.

Access to the EPS system is role based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Diplomatic Security (DS) Security Configuration Guides, and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor CA systems including this specific system.

Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with DS Configuration Guides, auditing is enabled to track the following events on the host operating systems and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

In accordance with Department of State computer security policies, mandatory security (PS800 Cyber Security Awareness) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. PA459 (Protecting Personally Identifiable Information) privacy training is required for all direct-hire employees accessing systems with PII.

(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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Resources Management Office, Information Integrity Branch (IIB) provides administrative life-cycle security protection guidelines for the Department of State's information technology systems and information resources. EPS must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security.

(f) How were the security measures above influenced by the type of information collected?
Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

System Administrators are responsible for all daily maintenance, establishing access control lists (ACLs), and backups. The duties of system administrators require that they be granted system administrator privileges to the respective application servers. The respective post representative authorizes the establishment, activation, modification, review, disabling, and removing of all

System Administrator accounts.

Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration, to the database. DBA access is controlled by the Integrated Services (IS) team through the use of ACLs as established by the system administrators. This System DBAs are authenticated using Windows operating system authentication.

Department of State CA/CST employees who are responsible for ensuring fees are paid for the services rendered also have access to data in the system.

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

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

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

Information is documented in the System Security Plan. The ESP Plan includes information regarding system access to data. The plan specifically addresses procedures regarding access to data in EPS.

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

No, all users will not have access to all data in EPS outside of administrators. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

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

EPS information is protected by multiple layers of security controls including network security, Department site physical security and management security including:

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented.

-Least Privileges, which are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access

records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII via dual factor authentication utilizing a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.