PRESIDIO TRUST

The Presidio Trust
PRIVACY IMPACT ASSESSMENT

Introduction

The Presidio Trust requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted.

Name of Project: Parking Payment Compliance Program
Department: Transportation
Date: 03/21/24
Point of Contact
Name: Emily Beaulac
Title: Transportation Operations Specialist
Email: ebeaulac@presidiotrust.gov
Phone: 415-961-7622
Address: 1750 Lincoln Blvd, SF, CA 94129

Section 1. General System Information

A. Is a full PIA required?

☑ Yes, information is collected from or maintained on

- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☑ All

No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

The purpose of this system is to verify parking payment receipt and provide notice to violators in public paid parking areas within Area B of the Presidio. Operators of vehicles parked in public parking areas that require payment ("Parkers") have the option of purchasing parking on their mobile device or at the on-site pay stations. Transactions are identified and digitally recorded by license plate number. To confirm compliance with the posted payment requirements ("Compliance"), License Plate Reader ("LPR") technology is used to scan plate numbers and identify whether the Parker has posted payment. An accompanying system is used to populate and print Notices of Parking Violation Fees ("Violations").

C. What is the legal authority?
A Federal law, Executive Order of the President (EO), or Presidio Trust requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.
Title I, Omnibus Parks Public Lands Act of 1996, Public Law 104-333.
The Presidio Trust maintains broad authority over management and use of Area B in the Presidio, in accordance with the Trust Act. These authorities include the collection of parking fees and assessment of additional fees for failure to comply with posted parking fees and time limits. Law enforcement power in the Presidio Area B is reserved to the United States Park Police (USPP). The Trust's management authorities include actions aimed at increasing parking fee compliance. Parking payment compliance duties are performed by the Presidio Trust's Parking Management Contractor, ACE Parking, in coordination and collaboration with the United States Park Police.

D. Why is this PIA being completed or modified?
Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

☑ New Information System
☑ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in the Presidio Trust Privacy and Cyber Security System of Record?

☑ Yes:
☐No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.
Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. A separate PIA should be conducted for each hosted application or subsystem that contains PII to ensure privacy implications are assessed. In any case, the GSS PIA must identify all hosted

applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Genetec AutoVu	Hardware and software to scan license plates	Yes	This system is scanning license plate numbers.
Android devices and printers	Handheld devices used to input and print notices	No	
Passport Enforcement	Software to issue notices, lookup past offenses, pay issued fines, and dispute Violations	Yes	A record of Violations issued are kept to identify repeat violators. If payment for the violation is not received within 10 days of issuance, DMV records are used to mail the registered owner a letter with a reminder and instructions.
PaybyPhone (separate adapted PIA)	Allow users to purchase parking online	Yes	Users create an account using their phone number and purchase parking sessions using their billing information.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?
The Trust will publish a SORN for this system.
☑Yes:
☐ No

H. Does this information system or electronic collection require an OMB Control Number?
The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

☐ Yes: *Describe*
☑ No

The Presidio Trust is not using the Parking Payment Compliance Program technologies to collect information from the public or in any manner that would trigger the requirements of the Paperwork Reduction Act. Any planned use of these technologies that falls outside the scope of this assessment will require a complete PIA exclusive to the Parking Payment Compliance Program technologies use and coordination with the Presidio Trust Senior Agency Officials for Privacy.

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.
Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

PII is only collected when a violation is issued or when a person pays for their violation fee or disputes their violation fee online. A PayByPhone adapted PIA detailing the process for paying for parking is also available for review.

☑ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☑ Credit Card Number
☐ Law Enforcement
☐ Education Information
☐ Emergency Contact

☐ Driver's License
☐ Race/Ethnicity
☐ Social Security Number (SSN)
☑Personal Cell Telephone Number
☐ Tribal or Other ID Number
☑Personal Email Address
☐ Mother's Maiden Name
☐ Home Telephone Number
☐ Child or Dependent Information
☐ Employment Information
☐ Military Status/Service
☑Mailing/Home Address
☑ Other: License plate number.

B. What is the source for the PII collected? Indicate all that apply.
Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

☑ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ Presidio Trust records
☐ Third party source
☑ State agency (DMV Records)
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.
Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

☐ Paper Format
☐ Email

☐ Face-to-Face Contact
☑ Website
☐ Fax
☐ Telephone Interview
☑ Information Shared Between Systems. *Describe:* The California DMV Pull system
☐ Other: *Describe*

D. What is the intended use of the PII collected?
Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.
PII is collected to process Parking Violation Fees. A record of violations associated with a license plate number are stored as records within the Passport Inc. Enforcement system. A violation contains the following information: a violation number, the date, location ("The Presidio"), license plate number, violation type, vehicle make & model, staff identification number (parking employee), and the payment amount. The recipient of a violation is provided with instructions to pay their violation fee online. When the violation recipient pays their fee online, the Passport system collects their name and email address. Passport uses vehicle registered owner data from the DMV to send delinquent letters after 10 days of violation issuance to those owners in an attempt to resolve the unpaid citation. Once a payment has been made or a delinquent letter has been sent, the contact information provided or DMV registered owner information is stored with the record of violation.

License Plate Numbers (LPNs) scanned during patrols are collected and stored for 24-hour in the Genetec AutoVu system. An image of each scanned LPN is stored to identify vehicles that have exceeded posted time restrictions. The Genetec AutoVu system will share any previous images captured in the last 24-hours with the employee conducting patrols. All images and records containing LPNs or digital images captured by LPR are purged after 24 hours.

E. With whom will the PII be shared, both within the Presidio Trust and outside the Presidio Trust? Indicate all that apply.
Indicate all the parties, both internal and external to the Presidio Trust, with whom PII will be shared. Identify other Presidio Trust offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

☑ Within the Presidio Trust: *Describe the office and how the data will be used.*
The Presidio Trust's Transportation Team will have access to the Passport Portal database of issued violations, delinquent letters, and disputes submitted by parkers.
Violation records include the data/time of issuance, parking zone number, vehicle make/model, license plate number, two photos taken by the Parking Compliance staff member, and the information provider by the parker if the violation has been paid (first and last name, mailing address). This information is also used to respond to disputes and as evidence if a repeat violator is not responsive after receiving multiple parking violations.
Delinquent letters contain the registered vehicle owner's home mailing address. A record of delinquent letters are kept as evidence and to respond to complaints from parkers that may claim they did not receive proper notice or instruction.
Dispute records include the parker's first and last name, address, phone number, license plate number, citation details, evidence/reasoning provided by the parker, and dispute status. Dispute records are kept to respond to disputes and identify patterns of an individual that continues to dispute their violations without sound evidence.

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☑ Contractor: *Describe the contractor and how the data will be used.*
Presidio-based ACE Parking employees, who perform the parking compliance work, will have access to the same information on the Passport Portal as the Presidio Trust. This ensures they can manage the program and respond to disputes and customer inquiries.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?
If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

☑ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
Users may use the on-site parking pay stations to purchase parking sessions. All parking pay stations accept credit cards and some parking pay stations take coins. Users must provide their license plate number to purchase parking at the pay station. The Presidio Trust and ACE Parking do not have access to the record of license plate numbers collected at the pay stations; these records are encrypted and stored by the pay station vendor, Flowbird.

The license plate numbers of those that pay for parking using their cell phone are encrypted and not share with the Presidio Trust or ACE parking. Parkers that have paid fines online through Passport's online system may stop Passport from collecting information through their Passport account by ceasing to use their services. Users can contact Passport to delete or modify certain account information by contacting Passport through email.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.
Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

☑ Privacy Act Statement: The Trust will publish a SORN for this system.

☑ Privacy Notice: *Describe each applicable format.*
Parkers that receive fines are directed to Passport's Privacy Policy:
https://www.passportinc.com/privacy-policy/

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).
Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).
All personal information will be collected under the terms set forth in Passport's Terms and Conditions and Privacy Policy, which each end user must accept prior to providing any information or taking any other action within the application. Pursuant to those policies, Passport will purge data according to the data retention period stated within this PIA unless a particular end user specifically requests the deletion of their records. If this deletion is requested, Passport will comply with the request, provided, however, that information required to complete a

payment transaction will be retained in Passport's system as required to maintain an accurate, complete, and auditable database of transactions.

I. Will reports be produced on individuals?
Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

☑ Yes: *What will be the use of these reports? Who will have access to them?*
☐ No

The Violations and disputes from a single license plate number are stored together in the Passport Inc. Enforcement software system. The report can be accessed by searching for the license plate number within the database. The intention of this report is to assist with responding to disputes and to identify and confirm non-compliant users so escalation measures can be taken.

Section 3. Attributes of System Data

A. How will data collected from sources other than Presidio Trust records be verified for accuracy?
Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.
Registered owner data is retrieved directly from the DMV within the state where the vehicle is registered. This data is only stored temporarily to support immediate processing of the delinquent letter. It is re-retrieved at each point in the workflow in which it is required. Key data that is required for processing payments is verified via an out-of-band process; i.e. email to verify the email address, text to verify the phone number, an authorization charge to verify card data.

B. How will data be checked for completeness?
Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.
Key PII fields are required data elements and accounts will not be established without the presence of those fields. Registered owner data that is received from the DMV in an incomplete state will be discarded.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

Registered owner data is re-retrieved when it is necessary for processing delinquent letters. Violator data collected as part of a payment is only processed once and retained as a record of that transaction; that data is not utilized in future transactions or for other purposes within the system. The Presidio Trust relies on the data that the DMV provides and has no way to verify its accuracy prior to issuing a Violation.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Presidio Trust Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

Type	Retention
Digital images associated with Violations or dispute	2 years
Records of Violations	2 years from issuance
Records of disputes	2 years from receipt of first disputes attempt
License plate numbers captured using LPR	24-hours
Images captured using LPR	24-hours

If an end user would like their information removed from the system, Passport will accommodate that request.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, records management policies, or standard operating procedures.

Data is disposed of and permanently deleted from the Passport Enforcement system according to the schedule above. LPR data is automatically disposed of and permanently deleted from the Genetec AutoVu system after 24-hours. ACE Parking and the Presidio Trust do not store any PII outside of these systems. The procedures for deleting data are documented in the Parking Payment Compliance Program Policy and Procedure.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.
Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Presidio Trust and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Presidio Trust.

Passport applications require user authentication for both end users and administrators. Actions and data access are restricted by role-based access controls at all stages of the information lifecycle. All authentication and access attempts are logged within an audit record that contains the user id of the authenticated entity. All requests to REST API calls are logged.

Genetec applications require user authentication. User accounts are unique and account privileges are set based on how they are required to use the system. User activities can be monitored with Activity trails. Activity trails can be generated based on user, time range, or activity type.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

☑ Yes: *Explanation* A record of previous issued violations is necessary to issue escalating fines wherein the fine amount increases with each issued fine. DMV registration information is necessary to mail the Parker the notice of violation and instructions on paying their fine. PII collected by Passport is necessary to process credit card transactions.

LPNs and images captured of LPNs must be stored for 24-hours to enforce time restricted parking.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?
Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☑ No

C. Will the new data be placed in the individual's record?
Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☑ No

D. Can the system make determinations about individuals that would not be possible without the new data?
Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☑ No

E. How will the new data be verified for relevance and accuracy?

Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.
License plate numbers scanned will auto-populate the appropriate fields on the Violation issued on-site by the compliance staff member. The staff member will visually confirm the plate numbers and take photos as a record.

F. Are the data or the processes being consolidated?
If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III.

☑ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*
Passport applications require user authentication for both end users and administrators. Actions and data access are restricted by role-based access controls.

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.
Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.

☑ Users
☑ Contractors
☐ Developers
☑ System Administrator
☐ Other: *Describe*
Users: The Presidio Trust's Transportation Team
Contractors: Passport Operations and Support team employees who act in a support role can access data via a back office administrative web application.

Access to the application is locked down with multi-factor authentication and strict role-based access controls.
System Administrator: Administrative roles will have the ability to enter or update PII data.

H. How is user access to data determined? Will users have access to all data or will access be restricted?
Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities section. For additional information, review NIST SP 800-53 and FedRAMP.
Actions and data access are restricted by role-based access controls.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?
☑ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*
ACE Parking will have access to the record of issued violations, delinquent letters, and submitted disputes.
☐ No

J. Is the system using technologies in ways that the Presidio Trust has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?
Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

☐ Yes. *Explanation*

☑ No

K. Will this system provide the capability to identify, locate and monitor individuals?
Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☑ Yes. *Explanation*
Passport applications require user authentication for both end users and administrators. Actions and data access are restricted by role-based access controls. All authentication and access attempts are logged within an audit record that contains the user id of the

authenticated entity. All requests to REST API calls are logged.
☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

N/A

M. What controls will be used to prevent unauthorized monitoring?
Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.
Passport's backend management tool, Operator Management ("OpsMan"), is user/role based -- with password protected access for every function and feature. Access to OpsMan requires a value username and password. The system also keeps an audit trail of all actions within the system. This records the action performed, date, and user. The system will also record reports run, searches performed (With search parameters) from a CSR perspective as well. Passport gives the Presidio Trust full discretion as to how it would like to manage its system and can limit access by the individual user or their role within the Presidio Trust's administration.

N. How will the PII be secured?
Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☐ Identification Badges

☐ Safes
☐ Combination Locks
☐ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☑ Password
☑ Firewall
☑ Encryption
☑ User Identification
☐ Biometrics
☑ Intrusion Detection System (IDS)
☑ Virtual Private Network (VPN)
☑ Public Key Infrastructure (PKI) Certificates
☐ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☑ Periodic Security Audits
☑ Backups Secured Off-site
☐ Rules of Behavior
☑ Role-Based Training
☑ Regular Monitoring of Users' Security Practices
☑ Methods to Ensure Only Authorized Personnel Have Access to PII
☑ Encryption of Backups Containing Sensitive Data
☑ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.
Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public.

An individual requesting access to their records should send a written inquiry to the System Manager noted above or to the Presidio Trust Privacy Act Officer. A Privacy Act request must

meet the requirements of 36 CFR 1008 (https://www.ecfr.gov/current/title-36/chapter-X/part-1008). The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR ACCESS" on both the envelope and letter. A request to access records must meet the requirements of 36 CFR 1008 and 36 CFR 1008.13 (https://www.ecfr.gov/current/title-36/section-1008.13)-.14, .16-.17.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?
This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.
The Presidio Trust's Information Technology (IT) department is responsible for assuring proper use of the data and for reporting any issues with privacy protected information. The IT department will require audits of Passport to ensure compliance up to once per year.

Section 5. Review and Approval

Reviewing Official

Name: Luke R. Donohue
Title: Director
Department of Administration
Phone: 415-497-0471 Email:ldonohue@presidiotrust.gov

Signature: LUKE DONOHUE Digitally signed by LUKE DONOHUE Date: 2024.03.21 14:50:01 -07'00' Date: _____