

concern Market Dominant product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3622, 39 U.S.C. 3642, 39 CFR part 3030, and 39 CFR part 3040, subpart B. For request(s) that the Postal Service states concern Competitive product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3632, 39 U.S.C. 3633, 39 U.S.C. 3642, 39 CFR part 3035, and 39 CFR part 3040, subpart B. Comment deadline(s) for each request appear in section II.

II. Docketed Proceeding(s)

1. *Docket No(s)*.: CP2024–130; *Filing Title*: USPS Notice of Amendment to Priority Mail & USPS Ground Advantage Contract 148, Filed Under Seal; *Filing Acceptance Date*: April 12, 2024;² *Filing Authority*: 39 CFR 3035.105; *Public Representative*: Jennaca D. Upperman; *Comments Due*: April 23, 2024.

This Notice will be published in the **Federal Register**.

Erica A. Barker,
Secretary.

[FR Doc. 2024–08466 Filed 4–19–24; 8:45 am]

BILLING CODE 7710–FW–P

POSTAL REGULATORY COMMISSION

[Docket Nos. MC2024–232 and CP2024–238; MC2024–233 and CP2024–239]

New Postal Products

AGENCY: Postal Regulatory Commission.

ACTION: Notice.

SUMMARY: The Commission is noticing a recent Postal Service filing for the Commission’s consideration concerning a negotiated service agreement. This notice informs the public of the filing, invites public comment, and takes other administrative steps.

DATES: *Comments are due*: April 24, 2024.

ADDRESSES: Submit comments electronically via the Commission’s Filing Online system at <http://www.prc.gov>. Those who cannot submit comments electronically should contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section by telephone for advice on filing alternatives.

FOR FURTHER INFORMATION CONTACT: David A. Trissell, General Counsel, at 202–789–6820.

SUPPLEMENTARY INFORMATION:

² Docket Nos. MC2024–124 and CP2024–130, USPS Notice of Filing Revised Financials for Priority Mail & USPS Ground Advantage Contract 148, with Portions Filed Under Seal, April 12, 2024 (Errata).

Table of Contents

- I. Introduction
- II. Docketed Proceeding(s)

I. Introduction

The Commission gives notice that the Postal Service filed request(s) for the Commission to consider matters related to negotiated service agreement(s). The request(s) may propose the addition or removal of a negotiated service agreement from the Market Dominant or the Competitive product list, or the modification of an existing product currently appearing on the Market Dominant or the Competitive product list.

Section II identifies the docket number(s) associated with each Postal Service request, the title of each Postal Service request, the request’s acceptance date, and the authority cited by the Postal Service for each request. For each request, the Commission appoints an officer of the Commission to represent the interests of the general public in the proceeding, pursuant to 39 U.S.C. 505 (Public Representative). Section II also establishes comment deadline(s) pertaining to each request.

The public portions of the Postal Service’s request(s) can be accessed via the Commission’s website (<http://www.prc.gov>). Non-public portions of the Postal Service’s request(s), if any, can be accessed through compliance with the requirements of 39 CFR 3011.301.¹

The Commission invites comments on whether the Postal Service’s request(s) in the captioned docket(s) are consistent with the policies of title 39. For request(s) that the Postal Service states concern Market Dominant product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3622, 39 U.S.C. 3642, 39 CFR part 3030, and 39 CFR part 3040, subpart B. For request(s) that the Postal Service states concern Competitive product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3632, 39 U.S.C. 3633, 39 U.S.C. 3642, 39 CFR part 3035, and 39 CFR part 3040, subpart B. Comment deadline(s) for each request appear in section II.

II. Docketed Proceeding(s)

1. *Docket No(s)*.: MC2024–232 and CP2024–238; *Filing Title*: USPS Request to Add Priority Mail USPS Ground Advantage Contract 218 to Competitive Product List and Notice of Filing Materials Under Seal; *Filing Acceptance*

¹ See Docket No. RM2018–3, Order Adopting Final Rules Relating to Non-Public Information, June 27, 2018, Attachment A at 19–22 (Order No. 4679).

Date: April 16, 2024; *Filing Authority*: 39 U.S.C. 3642, 39 CFR 3040.130 through 3040.135, and 39 CFR 3035.105; *Public Representative*: Jennaca D. Upperman; *Comments Due*: April 24, 2024.

2. *Docket No(s)*.: MC2024–233 and CP2024–239; *Filing Title*: USPS Request to Add Priority Mail Express, Priority Mail USPS Ground Advantage Contract 55 to Competitive Product List and Notice of Filing Materials Under Seal; *Filing Acceptance Date*: April 16, 2024; *Filing Authority*: 39 U.S.C. 3642, 39 CFR 3040.130 through 3040.135, and 39 CFR 3035.105; *Public Representative*: Jennaca D. Upperman; *Comments Due*: April 24, 2024.

This Notice will be published in the **Federal Register**.

Erica A. Barker,
Secretary.

[FR Doc. 2024–08553 Filed 4–19–24; 8:45 am]

BILLING CODE 7710–FW–P

PRESIDIO TRUST

Privacy Act of 1974; System of Records

AGENCY: The Presidio Trust.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Presidio Trust is issuing a public notice of its intent to establish an Automated License Plate Recognition Program, system of records. INTERIOR PRESIDIO TRUST/Department of Public Safety-01, Automated License Plate Recognition (ALPR) system.

DATES: This system of records is effective upon publication. New routine uses will be effective May 22, 2024.

ADDRESSES: You may send comments via email to the interim Privacy Officer, within Presidio Trust’s Department of Administration, Luke Donohue, LDonohue@presidiotrust.gov or via U.S. Mail 1750 Lincoln Blvd. San Francisco, CA, 94129.

FOR FURTHER INFORMATION CONTACT: Luke Donohue, interim Privacy Officer, Presidio Trust, 1750 Lincoln Blvd. San Francisco, CA, 94129, LDonohue@presidiotrust.gov, (415) 317–8910.

SUPPLEMENTARY INFORMATION: The Presidio Trust, Internal-01, is establishing Automated License Plate Recognition (ALPR) systems of records. The purpose of the Automated License Plate Recognition (ALPR) system is to provide law enforcement agencies and the Director of the Department of Public Safety with a tool to assist with

investigations and crime prevention. Additionally, vehicular behavior habits through its gates of entry can be observed. The Flock Safety ALPR technology captures images of license plates and stores the plate data along with the location and time of capture.

Flock Safety's system consists of cameras and a cloud-based computing system which captures a whole or partial license plate number as well as make, model, and color of the vehicle. All collected data is encrypted using AES-256 encryption with a secure cloud server. Flock Safety allows the customer to own the data collected; the information is not shared or sold with third parties. The images in the system are collected from areas visible to the public where there is no reasonable expectation of privacy. The data collected may include license plate (whole or partial) images, vehicle make/model/color, and a record of the date, time, and location when the image was collected. The system creates a searchable computerized database, segmented by customer, resulting from the Flock Safety ALPR cameras in use by Flock Safety customers. The Flock Safety cameras are installed in a position to capture the license plate area of the vehicle and are focused in such a manner, that avoids collecting unintended images such as the driver or pedestrian(s).

Individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. Individuals who enter onto Federal properties and public areas do not have a reasonable expectation of privacy. Presidio Trust areas may have signs posted that inform individuals of surveillance activities, but in many cases notice may not be provided, or consent obtained for images captured during law enforcement operations or activities.

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information, and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974. 45 U.S.C. 142(a)(2).

Flock Safety stores all collected data on a secured portal for 30 days on their cloud through Amazon Web Services (AWS) using AES256 bit encryption, which is one of the highest encryption protections in industry standards. All

information is encrypted in transit from camera to cloud storage and encrypted at rest in the cloud. Multi-factor secured VPN access is needed to use the secured off-site database.

SYSTEM NAME AND NUMBER:

Automated License Plate Recognition (ALPR) Program, Internal-01.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Presidio Trust, Department of Public Safety, 1750 Lincoln Blvd., San Francisco, CA 94129. *watchcenter@presidiotrust.gov*

SYSTEM MANAGER(S):

Director of Public Safety, Tomas Kaselionis, *tkaselionis@presidiotrust.gov* 1750 Lincoln Blvd. San Francisco, CA 94129.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title I, Omnibus Parks Public Lands Act of 1996, Public Law 104-333, 110 Stat. 4097. 54 U.S.C. 100704, Inventory and Monitoring Program; 54 U.S.C. 100707, Confidentiality of Information.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to provide the Director of the Department of Public Safety and law enforcement with a tool (the ALPR system) to assist with investigations and crime prevention.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The data collected by the system will be stored for the sole purpose of identifying the vehicles of individuals engaged in unlawful conduct. Data may be collected from Presidio Park Visitors, Presidio Trust Staff, and Presidio Park Residents and/or Commercial Tenants.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains records of license plate (whole or partial), vehicle make and model, capture time, capture network, capture camera, capture location (latitude, longitude) and image/s of the vehicle.

RECORD SOURCE CATEGORIES:

Authorized Trust staff can import the data from Flock Safety in three ways:

CSV—The authorized user can export a CSV file containing the plate (whole or partial), capture time, capture network, capture camera, capture location (latitude, longitude) and image file name for a specific time frame. The Plate State is not included nor is additional vehicle information such as make and model.

IMAGES only—zip file of JPG files only identifiable by matching file name from the CSV.

PDF Report—Created by (username), date created, search reason, single vehicle image, zoomed in LPR image, GPS Map of camera location, license plate state and number, date captured, camera, camera location, vehicle body, make and color. License plate images and affiliated data will be purged after a 30-day period.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Interior as a routine use pursuant to 5 U.S.C. 552a(b)(3) may be made to:

(1) The appropriate Federal, State, local or foreign agency responsible for obtaining information relevant for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order when Presidio Trust becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

(2) The U.S. Department of Justice or in a proceeding before a court or adjudicative body when:

(a) The United States, the Presidio Trust, or, when represented by the government, an employee of the Presidio Trust is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Presidio Trust determines that the disclosure is relevant and necessary to the litigation and is compatible with the purpose for which the records were compiled.

(3) To a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(4) To appropriate agencies, entities, and persons when:

(a) The Presidio Trust suspects or has confirmed that there has been a breach of the system of records

(b) The Presidio Trust has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, The Presidio Trust (including its information systems, programs, and operations), the Federal Government, or national security.

(c) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with The Presidio Trusts efforts to respond to the suspected or

confirmed breach or to prevent, minimize, or remedy such harm.

(5) To another Federal agency or Federal entity, when the Presidio Trust determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) Responding to a suspected or confirmed breach.

(b) Preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national or national security, resulting from a suspected or confirmed breach.

(6) To Contractors when the contractor is working on a contract, service, job, or other activity for the Agency and who have a need to have access to the information in performance of their duties or activities for the Agency. Recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. 552a(m).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system can be retrieved by an authorized user, either by querying within the application or generating a report. All functions and features are password protected, with multi-factor authorization. The physical security of the Flock Safety data center is managed by Amazon AWS data centers, using AES256 bit encryption, and physical access to the Flock Safety office is restricted to authorized personnel only. Additionally, The Information Security program at Flock Safety aligns with industry recognized security frameworks including: System and Organization Controls (SOC) 2 Type II, SOC 3 Type II, NIST Cybersecurity Framework, Cloud Security Alliance's Cloud Control Matrix, AWS Foundational Security Best Practices, and CIS AWS Foundations Benchmarks.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Flock Safety uses administrative, operational, technical, and physical safeguards to protect ALPR information from unauthorized access, use, destruction, modification, or disclosure. Access to the system is granted by an agency administrator (the Director of Public Safety) and is protected by Username, password, and multi-factor authentication.

Flock Safety gives the Presidio Trust full discretion as to how to manage its system and can limit access for the individual user or their role within the

Presidio Trust's administration. Furthermore, Flock Safety tracks all user activity within the system. In addition, system searches are strictly tracked and require the user to provide a reason for every inquiry. This limits misuse or abuse of the system. Monitoring and auditing usage of the system can be conducted by the agency administrator. All logins and queries will be stored and monitored including: Username, Date, Time, Purpose of query, License plate and other elements used to query the system.

These data points will be stored in the Flock Safety system, and periodic audits will be conducted according to the policies of each Flock Safety customer to ensure access was made by authorized persons for legitimate purposes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

V Flock Safety will store the data (data hosting) and ensure proper maintenance and security of data stored in their cloud-based system. Flock Safety will also oversee purging data at the end of the 30 days of storage. Multi-factor secured VPN access to database, and a secure off-site database are used. In the unlikely event of an information breach, all individuals who are believed to be affected or have their information compromised will be notified by the Flock Safety Chief Technology Officer (CTO) or Chief Product Office (CPO).

After the retention period has passed, temporary records are disposed of in accordance with the applicable records schedule and Presidio Trust policy. Data is automatically deleted after 30 day retention period. Records documenting incidents, investigations, or activities requiring retention as evidence are exported as a hashed copy and provided to the appropriate evidence custodian. Records may be retained and disposed of by a receiving agency pursuant to their applicable records schedule(s). Monitoring and auditing usage of the system can be conducted by the administrator, the Director of Public Safety.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Flock Safety uses administrative, operational, technical, and physical safeguards to protect ALPR information from unauthorized access, use, destruction, modification, or disclosure. The Information Security program at Flock Safety aligns with SOC 2 Type II, SOC 3 Type II, NIST Cybersecurity Framework, Cloud Security Alliance's Cloud Control Matrix, AWS

Foundational Security Best Practices, and CIS AWS Foundations Benchmarks.

Flock Quality Assurance: ALPR is automated. License plate images, and details of collection are included in the system without review. Although infrequent, license plate translation may be incomplete or inaccurate. Users will confirm the computer translation prior to taking any action based on ALPR results. Furthermore, Flock Safety cannot release any information collected in the Presidio without expressed consent from the Presidio Trust, Director of Public Safety, as per the contract agreement.

RECORD ACCESS PROCEDURES:

Some of the records in this system may be shared with the Incident Management, Analysis and Reporting System (IMARS) for criminal acts committed on National Park Service (NPS) lands and inside and on the perimeter of protected NPS facilities.

An individual requesting access to their records should send a written inquiry to the applicable System Manager or the Privacy Act Officer identified above. A Privacy Act request must meet the requirements of 36 CFR 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 1008.13–14, .16–17.

CONTESTING RECORD PROCEDURES:

An individual requesting amendment of their records should send a written request to the applicable System Manager or the Privacy Act Officer as identified above. Instructions for submitting a request for amendment of records are available on the Presidio Trust Privacy Act Requests website at <https://www.PresidioTrust.gov/privacy/privacy-act-requests>. Requests must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include 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 AMENDMENT" on both the envelope and letter. A request for amendment must meet the requirements of 36 CFR 1008 and 36 CFR 1008.18–19, .22, .24.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records about them should send a written inquiry to the applicable System Manager or the Privacy Act Officer as identified above. A Privacy Act request must meet the requirements of 36 CFR 1008. The request must include a general description of the records 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 INQUIRY" on both the envelope and letter. A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Luke Donohue,

Director of Administration.

[FR Doc. 2024–08473 Filed 4–19–24; 8:45 am]

BILLING CODE 4310–4R–P

RAILROAD RETIREMENT BOARD

Proposed Collection; Comment Request

In accordance with the requirement of section 3506 (c)(2)(A) of the Paperwork Reduction Act of 1995 which provides opportunity for public comment on new or revised data collections, the Railroad Retirement Board (RRB) will publish periodic summaries of proposed data collections.

Comments are invited on: (a) Whether the proposed information collection is necessary for the proper performance of the functions of the agency, including whether the information has practical

utility; (b) the accuracy of the RRB's estimate of the burden of the collection of the information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden related to the collection of information on respondents, including the use of automated collection techniques or other forms of information technology.

1. *Title and purpose of information collection:* Application for Employee Annuity Under the Railroad Retirement Act; OMB 3220–0002.

Section 2(a) of the Railroad Retirement Act (RRA) (45 U.S.C. 231a) provides for payments of age and service, disability, and supplemental annuities to qualified employees. An annuity cannot be paid until the employee stops working for a railroad employer. In addition, the age and service employee must relinquish any rights held to such jobs. A disabled employee does not need to relinquish employee rights until attaining Full Retirement Age, or if earlier, when their spouse is awarded a spouse annuity. Benefits become payable after the employee meets certain other requirements, which depend on the type of annuity payable. The requirements for obtaining the annuities are prescribed in 20 CFR 216 and 220.

To collect the information needed to help determine an applicant's entitlement to, and the amount of, an employee retirement annuity the RRB uses Forms AA–1, *Application for Employee Annuity*; AA–1d, *Application for Determination of Employee Disability*; G–204, *Verification of Workers Compensation/Public Disability Benefit Information*, and electronic Forms AA–1cert, *Application Summary and Certification*, AA–1sum, *Application Summary*, and AA–1 (internet), *Application for Employee Annuity*.

The AA–1 application process obtains information from an applicant about their marital history, work history, military service, benefits from other governmental agencies, railroad pensions and Medicare entitlement for either an age and service or disability annuity. An RRB representative interviews the applicant either at a field office, an itinerant point, or by telephone. During the interview, the RRB representative enters the information obtained into an on-line information system. Upon completion of

the interview, the on-line information system generates Form AA–1cert, *Application Summary and Certification*, or Form AA–1sum, *Application Summary*, a summary of the information that was provided for the applicant to review and approve. Form AA–1cert documents approval using the traditional pen and ink "wet" signature, and Form AA–1sum documents approval using the alternative signature method called Attestation. When the RRB representative is unable to contact the applicant in person or by telephone, for example, the applicant lives in another country, a manual version of Form AA–1 is used.

Form AA–1d, *Application for Determination of Employee's Disability*, is completed by an employee who is filing for a disability annuity under the RRA, or a disability freeze under the Social Security Act, for early Medicare based on a disability. Form G–204, *Verification of Worker's Compensation/Public Disability Benefit Information*, is used to obtain and verify information concerning a worker's compensation or a public disability benefit that is or will be paid by a public agency to a disabled railroad employee. Form AA–1 (internet) can be completed by the applicant and submitted through the RRB's website at www.rrb.gov. One response is requested of each respondent. Completion of the forms is required to obtain/retain a benefit. The RRB proposes no changes to Form AA–1, Form AA–1 (internet), and Form G–204. The RRB proposes a minor editorial change to Form AA–1cert and Form AA–1sum to correct the title of the RB–9 booklet. The RRB proposes minor changes to Form AA–1d:

- Section 1, General Instructions, the date is being updated to 06/06/23 in the 3rd paragraph.
- Section 7 question 38, The entry in parentheses associated with the question now reads (Do not include any self-employment, unemployment or sickness benefits.)
- Section 8 question 45, has been changed to: Are you filing a form AA–1, *Application for Employee Annuity*, in connection with this application?
- Section 12 of the form. Under the Receipt for your claim section, the last sentence should read: Offices are open to public 9:00 a.m. to 3:00 p.m., Monday through Friday, and closed Federal holidays.