POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated databases, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By customer name, customer ID(s), distinguished name, certificate serial number, receipt number, transaction date, and email addresses.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records related to Pending Public Key Certificate Application Files are added as received to an electronic database, moved to the authorized certificate file when they are updated with the required data, and records not updated within 90 days from the date of receipt are destroyed.

2. Records related to the Public Key Certificate Directory are retained in an electronic database, are consistently updated, and records are destroyed as they are superseded or deleted.

3. Records related to the Authorized Public Key Certificate Master File are retained in an electronic database for the life of the authorized certificate.

4. When the certificate is revoked, it is moved to the certificate revocation file.

5. The Public Key Certificate Revocation List is cut off at the end of each calendar year and records are retained 30 years from the date of cutoff. Records may be retained longer with customer consent or request.

6. Other records in this system are retained 7 years, unless retained longer by request of the customer.

7. Records related to electronic signatures are retained in an electronic database for 3 years.

8. Other categories of records are retained for a period of up to 30 days.

9. Driver's License data will be retained for 5 years.

10. COA and Hold Mail transactional data will be retained for 5 years.

11. Records related to Phone Verification/One-Time Passcode and Device Reputation assessment will be retained for 7 years.

12. Records collected for Identity Proofing at the Identity Assurance Level 2 (IAL–2), including ID document images, Identity Verification Attributes, and associated data will be retained up to 5 years, or as stipulated within Interagency Agreements (IAAs) with partnering Federal Agencies. Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals who need the information to perform their job and whose official duties require such access.

Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections.

Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof, hardware device. Activities are audited, and archived information is protected from corruption, deletion, and modification.

For authentication services and electronic postmark, electronic data is transmitted via secure socket layer (SSL) encryption to a secured data center. Computer media are stored within a secured, locked room within the facility. Access to the database is limited to the system administrator, database administrator, and designated support personnel. Paper forms are stored within a secured area within locked cabinets.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure and Record Access Procedures above.

NOTIFICATION PROCEDURES:

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name, address, email, and other identifying information.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

March 16, 2020, 85 FR 14982; December 13, 2018, 83 FR 64164; December 22, 2017, 82 FR 60776; August 29, 2014, 79 FR 51627; October 24, 2011, 76 FR 65756; April 29, 2005, 70 FR 22516.

Joshua J. Hofer,

Attorney, Ethics & Legal Compliance.

[FR Doc. 2021–27113 Filed 12–14–21; 8:45 am]

BILLING CODE P

POSTAL SERVICE

Product Change—Priority Mail Negotiated Service Agreement

AGENCY: Postal Service™.

ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.

DATES: *Date of required notice:* December 15, 2021.

FOR FURTHER INFORMATION CONTACT: Sean Robinson, 202–268–8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on November 22, 2021, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail Contract 729 to Competitive Product List.* Documents are available at *www.prc.gov,* Docket Nos. MC2022–22, CP2022–24.

Sean Robinson,

Attorney, Corporate and Postal Business Law.

[FR Doc. 2021–27162 Filed 12–14–21; 8:45 am]

BILLING CODE 7710–12–P

POSTAL SERVICE

Product Change—Priority Mail Negotiated Service Agreement

AGENCY: Postal Service™.

ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.

DATES: *Date of required notice:* December 15, 2021.