



POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service.

ACTION: Notice of modified systems of records.

SUMMARY: The United States Postal Service (USPS) is proposing to revise two Privacy Act Systems of Records. These updates are being made to streamline USPS' policy creation and review process, to enhance USPS' capacity for oversight and security in their eCommerce environments, and to support enhanced USPS IT search services.

DATES: These revisions will become effective without further notice on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless, in response to comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (uspsprivacyfedregnotice@usps.gov). To facilitate public inspection, arrangements to view copies of any written comments received will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or uspsprivacyfedregnotice@usps.gov.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records. The Postal Service is proposing

revisions to two existing systems of records (SOR) to streamline USPS' policy creation and review process, to enhance USPS' capacity for oversight and security in their eCommerce environments, and to support enhanced USPS IT search services

I. Background

This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records.

The Postal Service is proposing to modify two SORs to streamline USPS' policy creation and review process, to enhance USPS' capacity for oversight and security in their eCommerce environments, and to support enhanced USPS IT search services:

USPS SOR 550.000 Commercial Information Technology Resources-
Infrastructure

USPS SOR 550.100 Commercial Information Technology Resources-
Applications

These proposed changes are as follows:

In USPS SOR 550.000 Commercial Information Technology Resources-
Infrastructure:

1. One new purpose, 17.
2. One revision to existing category of records, 1.

In USPS SOR 550.100 Commercial Information Technology Resources-
Applications:

1. Two new purposes, 13 and 14.
2. Nine new categories of records, 15 through 23.

II. Rationale for Changes to USPS Privacy Act Systems of Records

To ensure fairness, efficiency, security, and legal compliance, the Postal Service promulgates several types of policy and procedural documents. Given the complexity and length these documents may present, creation and revision to these documents can be quite onerous, occupying employee attention that could be spent elsewhere.

The Postal Service therefore will implement a new tool to assist this process, simplifying the policy creation and revision process, ensuring accountability for document stakeholders, and providing a single application source to track policy documents throughout their lifecycle.

In addition, the Postal Service will implement a new application providing oversight into USPS employee activity relating to eCommerce, enabling accountability and auditing to meet compliance and organizational requirements.

Finally, the Postal Service will introduce new functionality to utilize Artificial Intelligence services to analyze possible technology issues and provide remediation.

III. Description of the Modified Systems of Records

Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions to this SOR has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect that this modified system of records will have any adverse effect on individual privacy rights. Accordingly, for the reasons stated above, the Postal Service proposes revisions included in this system of records presented in its entirety as follows:

SYSTEM NAME AND NUMBER:

550.000 Commercial Information Technology Resources- Infrastructure

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

All USPS facilities and contractor sites.

SYSTEM MANAGER(S) AND ADDRESS:

For records of computer access authorizations: Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To provide USPS employees, contractors, and other authorized individuals with hierarchical access to and accounts for commercial information technology resources administered by the Postal Service and based on least privileged access.
2. To facilitate a cohesive software experience and simplify ease of use by sharing user and application data across participating IT programs.
3. To authenticate user identity for the purpose of accessing USPS information systems.
4. To assess user attributes and assign related access privileges.
5. To authenticate suppliers and contractors and facilitate further access to downstream Postal Service information systems.
6. To provide active and passive monitoring of information systems, applications, software, devices, and users for information security risks.

7. To review information systems, applications, software, devices, and users to ensure compliance with USPS regulations.
8. To facilitate and support cybersecurity investigations of detected or reported information security incidents.
9. To administer programs, processes, and procedures to assess information security risks and to detect information security threats and vulnerabilities.
10. To provide tools and analytics for USPS employees and contractors to measure work productivity and improve efficiency.
11. To improve manager-subordinate relationships within their formal reporting structure through data-based insights generated from their own email and related electronic communications with subordinates.
12. To provide employees access to a large language model based chat assistant.
13. To associate chat assistant conversations with individual USPS employee users for quick response and recollection.
14. To identify trends in chat assistant conversations for model refinement.
15. To ensure the accuracy of responses provided by the chat assistant to the end user.
16. To voluntarily provide data generated from chat assistant conversations to large language models for future model training and development.
17. To provide user-associated incidents to Artificial Intelligence algorithms for analysis and remediation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals with authorized access to USPS computers, information resources, and facilities, including employees, contractors, business partners, suppliers, and third parties.

2. Individuals participating in web-based meetings, web-based video conferencing, web-based communication applications, and web-based collaboration applications.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. *Information System Account Access records*: Records relating to the access or use of an information system, application, or piece of software, including; Name, User ID, Email Address, User Type, User Role, Job Title, Department, Manager, Company, Street Address, State Or Province, Country Or Region, Work Phone Number(S), Employee Identification Number (EIN), Advanced Computing Environment (ACE) ID, License Information, Action Initiated, Datetime, User Principle Name, Usage Location, Alternate Email Address, Proxy Address, Age Group, IP Address, MAC Address, Password, Multi-Factor Authentication Credentials, Security Questions, Security Answers, Passcode, Geolocation Data, User Profile Picture, Picture Metadata, Information Technology Account Administration User Configuration Status, Supplier Credentials, Supplier Company Codes, Conditional Access Attributes, Last Sign-In Time, User Account Status, User Admin Status, Password Length Compliance, Password Strength, Number Of Installed External Apps, Less Secure Apps Access, Admin-Defined Name, Profile Name Status, Photo Storage Space Used, Total Storage Space Used, Storage Usage Percentage, Total Emails Sent, Total Emails Received, Total Emails Sent And Received, Email Server Last Usage Time, Device Application Change, Device Privilege Changed, Device Policy Changed, Device Action Reported, Device Compliance Status, Device Operating System Updated, Device Ownership Updated, Device Settings Changed, Device Status Changed Through Apple Device Enrollment, Device Account Synced, Device Risk Signal Updated, Device Work Profile Submitted, Document Uploaded to chat assistant,

Desk Location, District Code, Domain, Duty Finance Number, EDU Status, Employee Type, Enable Multifactor Authentication True/False, External User Type, Failed Login Attempts, Federated ID String, FLSA String, Gender, Geolocation tracked True/False, Hashed User ID String, Internal Integration User True/False, Language, Last Login Date, Last Login Device, Last Login Time, Last Password, Last position, Latitude Floating Point Number, LDAP Server, LDC Code, Location, Locked Out True/False, Longitude Floating Point, Mailer ID, Non-Assignable True/False, Notification Integer, Occupation Code, On Schedule Choice, Organization, Password Needs Reset True/False, Pay Band, Pay Band Level Code, Pay Location, PCES Manager True/False, PCI User True/False, Performance Cluster Code, Prefix, Schedule, Source, SSO Source, STAF Session, Sys ID, Time Format, Time sheet policy, Time Zone, Title, Updated Date/Time, Updated By, Updates, System Specific User ID, VIP True/False, VP Organization, Web Service Access Only True/False, Work Agent Status, VoicePrint.

2. *Security Analytics records*: Records relating to the gathering, analysis, review, monitoring, and investigation of information system security risks, including; User Investigation Priority Score, User Identity Risk Level, User Lateral Movement Paths, User Devices Numbers, User Account Numbers, User Resources Numbers, User Locations Numbers, User Matches Files Numbers, User Locations, Apps Used By User, User Groups, User Last Seen Date, User Affiliation, User Domain, App Instance, Organizational Groups, User Account Status, Activity ID, Activity Objects, Activity Type, Administrative Activity, Alert ID, Applied Action, Activity Date, Device Tag, Activity Files And Folders, Impersonated Activities, App Instance Activity, App Location Activity, Activity Matched Policy, Activity Registered ISP, Activity Source, Activity User, Activity

User Agent, Activity User Agent Tag, Application Risk Score, Application Activity, User Software Deactivation, User Software Installation, User Software Removal, Last Date Of Software Execution, Internet Application Transaction Counts, Data Volume Upload, Data Volume Download, Data Sensitivity Classification, Internet Protocol, Internet Port, And Internet Access History, Login IP Address, Login Type, Login Failed, Login Successful, Number Of Times A User Was Suspended, Number Of Times A User Was Suspended Due To Spam Relay, Number Of Times A User Was Suspended Due To Spam, Number Of Times A User Was Suspended Due To Suspicious Activity, Device Name, Device Operating System, Days Since First Sync, Days Since Last Sync, Device Status, Device Type, Device Model, Device Account Registration Changed, Device Action Event, Device Compliance Status, Device Compromise Status, Device Ownership Change, Device Operating System Updated, Device Settings Changed, Device Failed Screen Unlock Attempts, Device Status Changed On Apple Portal, Device User Signed Out, Device Suspicious Activity Detected, Device Work Profile Supported, Two-Factor Authentication Disabled, Two-Factor Authentication Enrolled, Account Password Changed, Account Recovery Email Changed, Account Recovery Phone Number Changed, Account Recovery Secret Question Changed, Account Recovery Secret Answer Changed, Account Password Leak Suspected, Account Suspicious Login Blocked, Account Suspicious Login From Less Secure App Blocked, Suspicious Programmatic Login Blocked, User Suspended, User Suspended (Spam Through Relay), User Suspended (Spam), User Suspended (Suspicious Activity), Account Enrolled In Advanced Protection, Account Unenrolled In Advanced Protection, Account Targeted By Government-Backed Attack, Out Of Domain Email Forwarding Enabled, Login Challenge Question Presented, Login Verification Presented, Log

Out, Secure Shell Public Key Added, Secure Shell Public Key Deleted, Secure Shell Public Key Retrieved, Secure Shell Public Key Updated, Login Profile Retrieved, POSIX Account Deleted, Application Method Called, Application Access Authorized, Application Access Revoked, Device Compromised, Failed Password Attempts On User Device, Device Property Changed.

3. *Productivity Analytics records*: Records relating to the gathering, analysis, review, and investigation of information system utilization, including; Calendar Appointments, Email Read Rate, Email Response Rate, Operating System Activity History, Email Timestamp, Statements Made In Email Body, Email Sender, Email Recipient, Email Subject Line, Calendar Event Type, Calendar Event Status, Calendar Event Category, Calendar Event Subject, Calendar Event Duration, Calendar Event Attendees, Meeting Organizer, Meeting Invitees, Meeting Subject Line, Meeting Scheduled Time, Meeting Attendee Status, Meeting Scheduled Location, Web Call Organizer, Web Call Invitees, Web Call Scheduled Time, Web Call Joined Time, Web Call Duration, Web Call Status, Web Call Join Status, Number Of Collaborative Audio Calls Made, Number Of Collaborative Video Calls Made, Chat Initiator, Chat Recipient, Chat IM Sent Time, Number Of Cloud-Based Personal Storage Documents Worked On, Number Of Cloud-Based Enterprise Storage Documents Worked On, Device Name, Chat Assistant Conversation Records, Chat Assistant Usage Metrics, Chat Assistant User Data.

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

Standard routine uses 1. through 9. apply. In addition:

a. To appropriate agencies, entities, and persons when (1) the Postal Service suspects or has confirmed that there has been a breach of the system of records;

(2) the Postal Service has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Postal Service (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Postal Service's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

RECORD SOURCE CATEGORIES:

Employees; contractors; customers.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

1. Records relating to information system access are retrievable by name, email address, username, geolocation data, and ACE ID.
2. Records relating to security analysis are retrievable by name, unique user ID, email address, geolocation data, IP address and computer name.
3. Records relating to productivity are retrievable by name, email address, and ACE ID.
4. Records relating to third-parties are retrievable by name, email address, user name, and IP address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records relating to information system access are retained twenty-four months after last access.
2. Records relating to security analysis are retained for twenty-four months.
3. Records relating to productivity are retained for twenty-four months.

4. Records relating to third-parties are retained for twenty-four months.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

Access to records is limited to individuals 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 encryption, 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.

NOTIFICATION PROCEDURE:

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the Chief Information Officer and Executive Vice President and include their name and address.

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.

EXEMPTION(S) PROMULGATED FROM THIS SYSTEM:

None.

HISTORY:

April 3, 2025; 90 FR 14666; May 10, 2021; 86 FR 24907.

SYSTEM NAME AND NUMBER:

550.100 Commercial Information Technology Resources—Applications.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

All USPS facilities and contractor sites.

SYSTEM MANAGER(S) AND ADDRESS:

For records of computer access authorizations: Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To provide event registration services to USPS customers, contractors, and other third parties.
2. To allow task allocation and tracking among team members.
3. To allow users to communicate by telephone, instant-messaging, and email through local machine and web-based applications on desktop and mobile operating systems.
4. To share your personal image via your device camera during meetings and web conferences, if you voluntarily choose to turn the camera on, enabling virtual face-to-face conversations.
5. To provide for the creation and storage of media files, including video recordings, audio recordings, desktop recording, and web-based meeting recordings.
6. To provide a collaborative platform for viewing video and audio recordings.

7. To create limited use applications using standard database formats.
8. To review distance driven by approved individuals for accurate logging and compensation.
9. To develop, maintain, and share computer code.
10. To comply with Security Executive Agent Directive (SEAD) 3 requirements for self-reporting of unofficial foreign travel pertaining to covered individuals who have access to classified information or who hold a sensitive position.
11. To administer and maintain a secure board portal software that provides leadership with instant access to information they need before, during and after meetings, making board and committee interactions more efficient and productive by promoting collaboration and information sharing among USPS Board of Governors (BOG) and Executive Leadership Team (ELT).
12. To facilitate the software component of USPS-sponsored voluntary mentorship programs.
13. To support the administration of policy creation and revision applications.
14. To provide oversight data for eCommerce application access.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals with authorized access to USPS computers, information resources, and facilities, including employees, contractors, business partners, suppliers, and third parties.
2. Individuals participating in web-based meetings, web-based video conferencing, web-based communication applications, and web-based collaboration applications.
3. USPS Board of Governors, administrators, and USPS Executive Leadership Team.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. *Third-party Information records*: Records relating to non-Postal, third-party individuals utilizing an information system, application, or piece of software, including: Third-Party Name, Third Party Date Request, Third Party Free Text, Guest User Information.

2. *Collaboration application records*: Records relating to web-conferencing and web-collaboration applications, including; Collaborative Group Names, Collaborative Group IDs, Action Name, Number Of Actions Sent, Number Of Action Responses, Employee Phone Number, Collaborative Group Chat History, Profile Information, Collaborative Group Membership, Contacts, Project Owner, Project Creator, Event Start Time, Event Status, Event Organizer, Event Presenter, Event Producer, Event Production Type, Event Recording Setting, Total Number Of Event Media Viewings, Number Of Active Users, Number Of Active Users In Collaborative Groups, Number Of Active Collaborative Group Communication Channels, Number Of Messages Sent, Number Of Calls Participated In, Last Activity Date Of A User, Number Of Guest Users In A Collaborative Group, Event Name, Event Description, Event Start Date, Event End Date, Video Platform Group Name, Video Platform Group Email Alias, Video Platform Group Description, Video Platform Group Classification, Video Platform Group Access Level, Video Platform Channel Name, Video Platform Channel Description, Video Platform Channel Access, Video Platform Live Event Recording, Total Number Of Video Conferences, Add Room Member To Collaborative Group, Attachment Downloaded From Collaborative Group, Attachment Uploaded From Collaborative Group, Direct Message Started From Collaborative Group, Invite Sent From Collaborative Group, Message Edited From Collaborative Group, Message Posted In Collaborative Group, Remove Room Member From Collaborative Group, Room Created In Collaborative

Group, Add Service Account Permission To Enterprise Collaborative Group, Remove Service Account Permission To Enterprise Collaborative Group, Added User To Enterprise Collaborative Group, Added User Role To Enterprise Collaborative Group, Removed User From Enterprise Collaborative Group, Request To Join Enterprise Collaborative Group, Approve Join Request From Enterprise Collaborative Group, Reject Join Request From Enterprise Collaborative Group, Invite User To Enterprise Collaborative Group, Accept Invitation For Enterprise Collaborative Group, Reject Invitation For Enterprise Collaborative Group, Revoke Invitation For Enterprise Collaborative Group, Join Enterprise Collaborative Group, Ban User Including With Moderation In Enterprise Collaborative Group, Unban User From Enterprise Collaborative Group, Add All Users In Domain For Enterprise Collaborative Group, Create Group In Enterprise Collaborative Group, Delete Group In Enterprise Collaborative Group, Create Namespace In Enterprise Collaborative Group, Delete Namespace In Enterprise Collaborative Group, Change Info Setting In Enterprise Collaborative Group, Add Info Setting In Enterprise Collaborative Group, Remove Info Setting In Enterprise Collaborative Group, Add Member Role In Enterprise Collaborative Group, Remove User Role In Enterprise Collaborative Group, Membership Expiration Added In Enterprise Collaborative Group, Membership Expiration Removed In Enterprise Collaborative Group, Membership Expiration Updated In Enterprise Collaborative Group, ACL Permission Changed In Collaborative Group, Collaborative Group Invitation Accepted, Join Request Approved, User Joined Collaborative Group, User Requested To Join Collaborative Group, Collaborative Group Basic Setting Changed, Collaborative Group Created, Collaborative Group Deleted, Collaborative Group Identity Setting Changed, Collaborative Group Info Setting

Added, Collaborative Group Info Setting Changed, Collaborative Group Info Setting Removed, Collaborative Group New Member Restriction Changed, Collaborative Group Post Reply Settings Changed, Collaborative Group Spam Moderation Settings Changed, Collaborative Group Topic Setting Changed, Collaborative Group Message Moderated, User Posts Will Always Be Posted, User Added To Collaborative Group, User Banned From Collaborative Group, User Invitation Revoked From A Collaborative Group, User Invited To Collaborative Group, User Join Request Rejected From A Collaborative Group, User Reinvited To Collaborative Group, User Removed From Collaborative Group, Call Event Abuse Report Submitted, Call Event Endpoint Left, Call Event Livestream Watched, Individual Form Response, Form Respondent Email Address, Whiteboard Software Updated, Whiteboard Reboot Requested, Whiteboard Export Requested, Attachment Deleted, Attachment Uploaded, Note Content Edited, Note Created, Note Deleted, Note Permissions Edited.

3. Communication Application Records: Enterprise Social Network User Name, Enterprise Social Network User State, Enterprise Social Network User State Change Date, Enterprise Social Network User Last Activity Date, Number Of Messages Posted By An Enterprise Social Network User In Specified Time Period, Number Of Messages Viewed By An Enterprise Social Network User, Number Of Liked Messages By An Enterprise Social Network User, Products Assigned To A Enterprise Social Network User, Home Network Information, External Network Information, External Network Name, External Network Description, External Network Image, Network Creation Date, Network Usage Policy, External Network User Name, External Network User Email Address, External Group Name, Number Of Users On A Network, Network ID, Live Event Video Links, Files Added Or Modified In Enterprise Social Network, Message ID,

Thread ID, Message Privacy Status, Full Body Of Message, Chat User Action, Chat Room Member Added, Chat Attachment Downloaded, Chat Attachment Uploaded, Chat Room Blocked, Chat User Blocked, Chat Direct Message Started, Chat Invitation Accepted, Chat Invitation Declined, Chat Invitation Sent, Chat Message Edited, Chat Message Posted, Chat Room Member Removed, Chat Room Created.

4. *Multimedia records*: Records relating to media associated with or originating from an information system, including; Video Platform User ID, Video Name, Videos Uploaded By User, Videos Accessed By User, Channels Created By User, User Group Membership, Comments Left By User On Videos, Screen Recordings, Video Transcript, Deep Search Captions, Video Metadata, Audio Metadata, Phone Number, Time Phone Call Started, User Name, Call Type, Phone Number Called To, Phone Number Called From, Called To Location, Called From Location, Telephone Minutes Used, Telephone Minutes Available, Charges For Use Of Telephone Services, Currency Of Charged Telephone Services, Call Duration, Call ID, Conference ID, Phone Number Type, Blocked Phone Numbers, Blocking Action, Reason For Blocking Action, Blocked Phone Number Display Name, Date And Time Of Blocking, Call Start Time, User Display Name, SIP Address, Caller Number, Called To Number, Call Type, Call Invite Time, Call Failure Time, Call End Time, Call Duration, Number Type, Media Bypass, SBC FQDN, Data Center Media Path, Data Center Signaling Path, Event Type, Final SIP, Final Vendor Subcode, Final SIP Phrase, Unique Customer Support ID.

5. *Limited Use Application records*: Records relating to applications with a specific, limited use, including; Application Authoring Application Name, Application Authoring Application Author, Voice Search Text Strings, Miles

Driven, Mileage Rates, Country Currency, Destination, Destination Classification, Car Make, Car Model, Working Hours, Total Number Of Monthly Drives, Total Number Of Monthly Miles, Total Number Of Personal Drives, Total Number Of Personal Drives, Users Allowed To Access Application, Application Authoring Application Security Settings, Total Number Of Cloud-Based Searches Performed, Total Number Of Cloud-Based Search Queries From Web Browsers, Total Number Of Cloud-Based Search Queries From Android Operating Systems, Total Number Of Cloud-Based Search Queries From iOS Operating Systems, Data Visualization Report Email Delivery Added, Data Visualization Asset Created, Data Visualization Data Exported, Data Visualization Asset Deleted, Data Visualization Report Downloaded, Data Visualization Asset Edited, Data Visualization Asset Restored, Data Visualization Report Email Delivery Stopped, Data Visualization Asset Trashed, Data Visualization Report Email Delivery Updated, Data Visualization Asset Viewed, Data Visualization Link Sharing Access Type Changed, Data Visualization Link Sharing Visibility Changed, Data Visualization User Sharing Permissions Changed.

6. *Development Records*: Records relating to applications used for the creation, sharing, or modification of software code, including: Data Repository User ID, Data Repository Password, Data Repository User Address, Data Repository Payment Information, Data Repository User First Name, Data Repository User Last Name, Data Repository Profile Picture, Data Repository Profile Biography, Data Repository Profile Location, Data Repository User Company, Data Repository User Preferences, Data Repository User Preference Analytics, Data Repository Transaction Date, Data Repository Transaction Time, Data Repository Transaction Amount Charged, Data Repository web pages Viewed, Data Repository Referring website, Data Repository Date Of web page Request,

Data Repository Time Of web page Request, Data Repository User Commits, Data Repository User Commit Comment Body Text, Data Repository Pull Request Comment Body Text, Data Repository Issue Comment Body Text, Data Repository User Comment Body Text, Data Repository User Authentication, Language Of Device Accessing Data Repository, Operating System Of Device Accessing Data Repository, Application Version Of Device Accessing Data Repository, Device Type Of Device Accessing Data Repository, Device ID Of Device Accessing Data Repository, Device Model Of Device Accessing Data Repository, Device Manufacturer Of Device Accessing Data Repository, Browser Version Of Device Accessing Data Repository, Client Application Information Of Device Accessing Data Repository, Data Repository User Usage Information, Data Repository Transactional Information, Data Repository API Notification Status, Data Repository API Issue Status, Data Repository API Pull Status, Data Repository API Commit Status, Data Repository API Review Status, Data Repository API Label, Data Repository API User Account Signin Status, Data Repository API Schedule Status, Data Repository API Schedule List.

7. Unofficial Foreign Travel Monitoring: Records relating to covered individuals for the administration of the SEAD 3 program, including: Title, Name Of Traveler, Information Type: Pre-Travel And Post-Travel, Start Date Of Travel, End Date Of Travel, Carrier Of Transportation, Countries You Are Visiting, Passport Number, Passport Expiration Date, Names And Association Of Foreign National Travel Companions, Planned Foreign Contacts, Emergency Contact Name, Emergency Contact Phone Number, Emergency Contact Relationship, Post-Travel Questions Relating To Activity, Events, And Interactions.

8. Cloud-based storage records: Records relating to activity within cloud-based storage systems, including: Number Of Files Made Publicly Available, Number Of

Files Made Available With A Link, Number Of Files Shared With Domain Users, Number Of Files Shared With Domain Users Through Link, Number Of Files Shared With Users Outside Domain, Number Of Files Shared With User Or Group In Domain, Number Of Files Not Shared At All, Number Of Spreadsheet Documents Added, Number Of Text Documents Added, Number Of Presentation Documents, Number Of Form Documents Added, Number Of Other Files Added, Number Of Files Edited, Number Of Files Viewed, Number Of Files Added, Total Cloud Storage Space Used, Last Time Storage Accessed By User, Item Added To Folder, Item Approval Cancelled, Comment Added On Approval Of Item, Due Date Time Change Requested, Item Approval Requested, Reviewer Change Requested For Item Approval, Item Approval Reviewed, Document Copy Created, Document Created, Document Deleted, Document Downloaded, Document Shared As Email Attachment, Document Edited, Label Applied, Label Value Changed, Label Removed, Item Locked, Item Moved, Item Previewed, Item Printed, Item Removed From Folder, Item Renamed, Item Restored, Item Trashed, Item Unlocked, Item Uploaded, Item Viewed, Security Update Applied To File, Security Update Applied To All Files In Folder, Publish Status Changed, Editor Settings Changed, Link Sharing Access Type Changed, Link Sharing Access Changed From Parent Folder, Link Sharing Visibility Changed, Link Sharing Visibility Changed From Parent Folder, Security Update Removed From File, Membership Role Changed, Shared Storage Settings Changed, Spreadsheet Range Enabled, User Sharing Permissions Changed, User Sharing Permissions Changed From Parent Folder, User Storage Updated, File Viewed, File Renamed, File Created, File Edited, File Previewed, File Printed, File Updated, File Deleted, File Uploaded, File Downloaded, File Shared.

9. *Email Application records*: Records relating to regular use of email applications, including: Email Body Text, Email Metadata, Total Number Of Emails Sent, Total Number Of Emails Received, Total Number Of Emails Sent And Received, Last Time User Accessed Email Client Through A Post Office Protocol (POP) Mail Server, Last Time User Accessed Email Client Through An internet Message Access Protocol (IMAP) Mail Server, Last Time User Accessed Through Web-Based Server, Total Email Client Storage Space Used, Calendar Access Level(S) Changed, Calendar Country Changed, Calendar Created, Calendar Deleted, Calendar Description Changed, Calendar Location Changed, Calendar Time zone Changed, Calendar Title Changed, Calendar Notification Triggered, Calendar Subscription Added, Calendar Subscription Deleted, Calendar Event Created, Calendar Event Deleted, Calendar Event Guest Added, Calendar Event Guest Auto-Response, Calendar Event Guest Removed, Calendar Event Guest Response Changed, Calendar Event Modified, Calendar Event Removed From Trash, Calendar Event Restored, Calendar Event Start Time Changed, Calendar Event Title Modified, Successful Availability Lookup Of A Calendar Between Email Clients, Successful Availability Lookup Of Email Client Resource, Successful Email Client Resource List Lookup, Unsuccessful Availability Lookup Of A Calendar On Email Client, Unsuccessful Availability Lookup Of Email Client Resource, Unsuccessful Email Client Resource List Lookup.

10. *Web Browser Records*: Records relating to activity within a web browser, including: Web Browser Password Changed, Web Browser Password Reused, Malware Detected in Transferred Content for User, Sensitive Data Detected In Transferred Content, Unsafe website Visit Detected For User.

11. USPS Board of Governors name, email, and collaborative meeting records used to store meeting material such as presentations, briefing documents/memos, meeting minutes/notes, and responses to various board inquiries, presentation briefing documents, and memos.

12. Mentorship Application Information: Match Data Stored About A User, Program Membership Status, Program Eligibility, Program Enrollment Date, Program Participation Preference, Mentor / Mentee Capacity, Preferred Mentors, Accepting New Matches Status, Recommended Mentors, Declined Recommendation Reason, Active Mentor/Mentee/Peer Relationships, Relationship Start / End Date, User Who Requested The Relationship, Relationship Status, Action Item / Checklist Item Progress, Mentorship Agreements, Pairing Health, Mentor/Mentee/Peer Relationship Requests, Mentor/Mentee/Peer Relationship Extension Requests, Mentor/Mentee/Peer Request Introduction Notes, Mentor/Mentee/Peer Request Preferred Match Duration, Past Mentor/Mentee/Peer Relationships, Active Group Membership As A Mentor/Mentee/Peer, Group Name, Group Start / End Date, Group Status, Past Group Membership As A Mentor/Mentee/Peer.

13. Mentoring Session Data Stored For A User: Status, Default Admin Agenda, Custom User Agenda, Start / End Date Time, Mentee/Mentor Feedback, 1-4 Star Rating, Free Text Session Feedback, Private Session Notes, Shared Session Notes, User Booking Session, Session Calendar Event And Videoconferencing Details, Session Attendance, Session Topics.

14. Program Survey Data Stored For A User: Survey Status, Custom Admin Supplied Question Responses, Program Admin Data, Reporting Column Preferences, Program Admin Support Contact.

15. Policy Document Report records: Document Title, Reference Number, Document Category, Related Documents, Document Content, Document Owner, Document Issue Date, Document Availability, Related Policy, Summary of Major Changes, Executive Leadership Team (ELT) Sponsor.

16. Policy Crosswalk and accountability records: Former Language, Revised Language Document, Revised Language Location in Document, Reason for Change, Anticipated Impact on Bargaining Employees, Decision Approver, Date of Decision.

17. Policy document Approval records: Active Approval Query, Approval, Approval For, Approval Journal Column, Approval source, Approver Reference, Approving Document ID, Comments, Created Date, Created By, Deferral Reason, Due date, Domain, Domain Path, Expected start, GRC approval level, Group, Iteration, Level, Order, Policy Name, Process step, Register account, Register email, Register name, Rejection Reason, Source table, State binding, System State, Status, Sys ID, Updated Date, Updated By, Updates, Users, Workflow activity.

18. Policy document table records: Active, Additional comments, Additional information, Allow users to decline, Allow users to request exceptions, Approval method, Approval rule, Approvers, Attestation, Audience, Category, Class, Classification, Compliance score (%), Connect document, Created Date/Time, Created By, Day of the month, Day of week, Description, Document Contributors, Document text, Domain, Domain Path, Enable redlining, First Acknowledgement Date, Frequency, Functional domain, Has downstream controls, Imported, Published policy, Last sync date, Maximum exception duration (days), Policy Name, Next Acknowledgement Date, Policy Number, Number of days to respond, Owner, Owning group, Parent, Policy categories, Policy knowledge

base, Policy Template, Provider, Publish count, Redlining state, Reference Material URL, Reviewers, Source, Source ID, Source last modified Date, Source release version, Source version, State, Sys ID, Type, Updated Date, Updated By, Updates, Valid from Date, Valid to Date, 508 Compliance Specialist, Corporate Policy Management, Crosswalk, Deputy PMG/Chief Human Resources Officer, Document Lead, Document Link URL, Document Owner(s), ELT Alignment, Executive Leadership Team, Executive Leadership Team (ELT) Sponsor, General Counsel, Labor Relations Point of Contact, Law Department Point of Contact, Notice of Retirement URL, PMG/Delegates List, Reference ID, Sharepoint Folder URL, Track Changes Document URL, VP Alignment.

19. Compliance Request Table record: Active, Activity Due Date, Additional assignee List, Additional comments, Additional source, Allowed groups, Allowed users, Approval, Approval Date, Approval History, Approved on Date, Approvers, Assigned To, Assignment Group, Attachment, Business Application, Business Duration, Business Service, Case closure SLA, Closed Date, Closed By, Comments And Work Notes, Company, Confidential True/False, Configuration Item, Contact Type, Contract, Correlation Display, Correlation ID, Created Date, Created By, Date Submitted, Delivery Plan, Delivery Task, Description, Domain, Due Date, Duration, Effective number, Date Due, Determination, Escalation, Expected Start Date, Follow Up Date, Group List, Impact, Impacted business unit, Impacted department, Knowledge, Location, Made SLA True/False, Number, Opened By, Order, Parent, Primary entity, Priority, Product CI, Reassignment Count, Rejected on Date, Rejection Goto, Requested on behalf of, Resolved, Reviewers, Service, Service CI, Service offering, Short Description, Skills, SLA Due, Source, Source record, Source table, Start Date, State model, Status, Sub-location, Sub-type, Substate, Sys ID, Task Type, Template, Time

Worked, Transfer reason, Type, Universal Request, Updated, Updated By, Updates, Upon Approval, Upon Reject, Urgency, User Input, Variables, Watch List, Work Notes, Work Notes List, Workflow Activity.

20. Policy Document Action Task records: Accepted date, Active, Activity Due Date, Additional assignee list, Additional Comments, Approval, Approval Date, Approval History, Assessment Template, Assigned To, Assignment Group, Attachment, Business Application, Business Duration, Business Service, Closed Date, Closed By, Comments And Work Notes, Company, Configuration Item, Contact Type, Contract, Correlation Display, Correlation ID, Created Date, Created By, Date, Delivery, Delivery Task, Description, Domain, Domain Path, Due date, Duration, Effective number, Due Date, Escalation, Expected Start Date, Follow Up Date, Group List, Impact, Is data present, IT asset, Knowledge, Location, Made SLA, Number, Observations, Opened By, Order, Origin, Parent, Priority, Product CI, Reassignment Count, Rejection Goto, Resolved Note, Service, Service CI, Service offering, Short Description, Skills, SLA Due Date, Start Date, State model, Status, Sys ID, Task Type System, Template, Time Worked, Transfer, Type, Universal Request, Updated Date, Updated, Updates, Upon Approval, Upon Reject, Urgency, User Input, Variables, Document Reviewer Watch List, Work Notes, Work Notes, Workflow Activity, Approval Notification, Capture function or administrative realignments, Capture organizational title changes, Clarify "must-do's" and reduce low value-added work, Clarify roles and responsibilities, Comply with statutory, regulatory, contractual changes, or audit recommendation, Consolidate in parts into another document; rest can be retired, Define purpose, scope and audience for new policy, process or procedure, Determine related documents, and if they need to be created or updated, Determine roles and responsibilities for new policy,

process or procedure, Enhance strategic alignment or close gap to commercial or other best practice, Establish only "must do's" and guardrails in new policy, process or procedure, Insert details or examples, Insert details or examples, and list sections, Insert name(s) of document(s) that supersede this document, Interdependencies with other policies or related documents, List document(s) name(s) and list all parts that were, Major modifications to document, Major risks and mitigation, Movement of content from another document, Obsolete in its entirety, Other, Rationale for Update, Retire, or New, Reflect operational or technological changes, Select the required level of change to the document, Separate policy and process instructions, Streamline and simplify structure and language, Summary of current policy or related document, or a proposed new document, Supersedes in its entirety by another policy, process or procedure, Value generated through Updated, Retired, or New document.

21. Document Task Records: Active, Activity Due Date, Additional assignee list, Additional comments, Approval, Approval Date, Approval History, Assigned To, Assignment Group, Attachment, Business Application, Business Duration, Business Service, Closed Date, Closed By, Comments And Work Notes, Company, Configuration Item, Contact Type, Contract, Correlation Display, Correlation ID, Created Date, Created By, Date Submitted, Delivery Plan, Delivery Task, Description, Domain, Due date, Duration, Effective number, Date due, Escalation, Expected Start Date, Follow Up Date, Group List, Impact, Knowledge, Location, Made SLA, Number, Opened By, Order, Parent, Priority, Product, Reassignment Count, Rejection Goto, Resolved Note, Service, Service CI, Service offering, Short Description, Skills List, SLA Due Date, Start Date, Status, Sys ID, Task Type, Template, Time Worked, Transfer reason, Universal Request, Updated Date, Updated By, Updates, Upon Approval, Upon Reject,

Urgency, User Input, Variables, Watch List, Work Notes, Work Notes List, Workflow Activity, Action item, Date Briefing Occurred, Document task type, Document Title.

22. Related Area Update Records: Case, Created Date, Created By, Description, Domain, Domain Path, Related Area, Related area table, Related area type, Sys ID, Title, Type, Updated Date, Updated By, Updates.

23. eCommerce Application Oversight Records: User Email Address, User ACE Credentials, Event Timestamp, Managed Host Domain, Managed Application ID, Managed Web Page, Script/Header Status Updated, Script/Header Note Created, Script Justification Created/Updated/Deleted, Policy Rule Created/Activated/Modified/Archived, Policy Rule Priority Set/Changed, Script/Action/Incident Added/Removed From Allow/Deny List, Incident Moved to Under Review, Email Integration Created/Updated/Deleted, 3rd Party Tool Integration Created/Updated/Deleted, API Token Created/Deleted, Alert Group Created/Updated/Deleted, Account Created/Updated/Deleted, User Created/Updated/Deleted, User Role Assigned/Changed/Deleted, Custom Role Created/Updated/Deleted, Vendor Tag Created/Updated/Deleted.

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

Standard routine uses 1. Through 9. Apply. In addition:

- a. To appropriate agencies, entities, and persons when (1) the Postal Service suspects or has confirmed that there has been a breach of the system of records; (2) the Postal Service has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Postal Service (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to

such agencies, entities, and persons is reasonably necessary to assist in connection with the Postal Service's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

RECORD SOURCE CATEGORIES:

Employees; contractors; customers; USPS Board of Governors.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

1. Records relating to third-parties are retrievable by name and email address.
2. Records relating to collaboration are retrievable by name, email address, and user ID.
3. Records relating to communication are retrievable by name, email address, and user ID.
4. Records pertaining to multimedia are retrievable by username and media title.
5. Records relating to application development are retrievable by user ID and application name.
6. Records relating to limited use applications are retrievable by name, email address, and user ID.
7. Records relating to Unofficial Foreign Travel Monitoring for covered individuals are retrievable by name.
8. Records relating to Cloud-based storage are retrievable by name, email address, and user ID.
9. Records relating to Email Applications are retrievable by name, email address, and user ID.

10. Records relating to Web Browsers are retrievable by name, email address, and user ID.

11. USPS Board of Governors secure board portal collaboration software data is retrievable by date, meeting information, committee name, and other session collaboration details.

12. Records relating to mentorship programs are retrievable by mentee name

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS:

1. Records relating to third parties are retained for twenty-four months.

2. Records relating to collaboration are retained for twenty-four months.

3. Records relating to communication are retained for twenty-four months.

4. Multimedia recordings are retained for twenty-four months.

5. Records relating to application development are retained for twenty-four months.

6. Records relating to limited use applications are retained for twenty-four months.

7. Records relating to Unofficial Foreign Travel Monitoring for covered individuals are retained for twenty-five years.

8. Records relating to Cloud-based storage are retained for twenty-four months.

9. Records relating to Email Applications are retained for twenty-four months.

10. Records relating to Web Browsers are retained for twenty-four months.

11. USPS Board of Governors secure board portal collaboration software data is retained up to twelve months from the close of the corresponding event.

12. Records relating to mentorship programs are retained for twenty-four months.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

Access to records is limited to individuals 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 encryption, 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.

NOTIFICATION PROCEDURE:

Customers and employees wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the Chief Information Officer and Executive Vice President and include their name and address.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure 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.

EXEMPTION(S) PROMULGATED FROM THIS SYSTEM:

None.

HISTORY:

April 16, 2025; 89 FR 26953; December 1, 2023; 88 FR 83981; May 11, 2021; 86 FR 25899; January 31, 2022; 87 FR 4957.

Daria Valan,

Attorney, Ethics and Legal Compliance.

[FR Doc. 2026-00250 Filed: 1/8/2026 8:45 am; Publication Date: 1/9/2026]