**P**

**Privacy Act; System of Records**

**AGENCY:** Postal Service™.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** The United States Postal Service™ (USPS™) is proposing to revise one General and one Customer Privacy Act Systems of Records. These updates are being made to support an initiative to implement a platform to manage Application Program Interfaces (APIs).

**DATES:** These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**], unless 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). Arrangements to view copies of any written comments received, to facilitate public inspection, will be made upon request.

**FOR FURTHER INFORMATION CONTACT:** Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office at uspsprivacyfedregnotice@usps.gov or 202-268-2000.

**SUPPLEMENTARY INFORMATION:**

**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 the following SORs to implement a platform to manage APIs:

- USPS SOR 550.200 Commercial Information Technology Resources-Administrative
- USPS SOR 830.000 Customer Service and Correspondence

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

Versatility and manageability are integral components of an organization's technology infrastructure. Application Programming Interfaces (APIs) allow applications to coordinate, send, and process data between otherwise disparate applications. The Postal Service utilizes a variety of these APIs for numerous reasons; however, the number and deployability of these APIs within the Postal Service's technology ecosystem can prove onerous. To that end, the Postal Service intends to implement an API manager for a limited scope. The scope of this new application will manage APIs connected or associated with an existing customer relationship management application. To achieve this effort, the systems of records will be revised as follows:

- USPS SOR 550.200 Commercial Information Technology Resources- Administrative will be revised to modify one existing category of records, and will add fifteen new categories of records to reflect the auditing and tracking capabilities of users of the API manager.
- USPS SOR 830.000 Customer Service and Correspondence will be revised with one new purpose to allow the transmission of data to the API manager and to the ultimate destination of that customer data.

**III. Description of the Modified System 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 has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect these amended systems of records to have any adverse effect on individual privacy rights. The notices for USPS SOR 550.200 Commercial Information Technology Resources- Administrative and USPS SOR 830.000 Customer Service and Correspondence are provided below in their entirety:

**SYSTEM NAME AND NUMBER:**

550.200 Commercial Information Technology Resources- Administrative

**SECURITY CLASSIFICATION:**

None.

**SYSTEM LOCATION:**

All USPS facilities and contractor sites.

**SYSTEM MANAGER(S):**

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 active and passive monitoring and review of information system applications and user activities.
2. To generate logs and reports of information system application and user activities.
3. To provide a means of auditing commercial information system activities across applications and users.

**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. General Audit Log activities: DateTime, IP Address, User Activity, User Item Accessed, Activity Detail, Object ID, Record Type, Client IP Address, CorrelationID, CreationTime, EventData, EventSource, ItemType, OrganizationID, UserAgent, USerKEy, UserType, Version, Workload.
2. File and page activities: Accessed file, Change retention label for a file, Deleted file marked as a record, Checked in file, Changed record status to locked, Changed

record status to unlocked, Checked out file, Copied file, Discarded file checkout, Deleted file, Deleted file from recycle bin, Deleted file from second-stage recycle bin, Detected document sensitivity mismatch, Detected malware in file, Deleted file marked as a record, Downloaded file, Modified file, Moved file, Recycled all minor versions of file, Recycled all versions of file, Recycled version of file, Renamed file, Restored file, Uploaded file, Viewed page, View signaled by client, Performed search query.

3. Folder activities: Copied folder, Created folder, Deleted folder, Deleted folder from recycle bin, Deleted folder from second-stage recycle bin, Modified folder, Moved folder, Renamed folder, Restored folder.
4. Cloud-based Enterprise Storage activities: Created list, Created list column, Created list content type, Created list item, Created site column, Created site content type, Deleted list, Deleted list column, Deleted list content type, Deleted list item, Deleted site column, Deleted site content type, Recycled list item, Restored list, Restored list item, Updated list, Updated list column, Updated list content type, Updated list item, Updated site column, Updated site content type.
5. Sharing and access request activities: Added permission level to site collection, Accepted access request, Accepted sharing invitation, Blocked sharing invitation, Created access request, Created a company shareable link, Created an anonymous link, Created secure link, Deleted secure link, Created sharing invitation, Denied access request, Removed a company shareable link, Removed an anonymous link, Shared filer, folder, or site, Unshared file folder or site, Updated access request, Updated an anonymous link, Updated sharing invitation, Used a company shareable link, Used an anonymous link, Used secure link, User added to secure link, User removed from secure link, Withdrew sharing invitation.
6. Synchronization activities: Allowed computer to sync files, Blocked computer from syncing files, Downloaded files to computer, Downloaded file changes to computer, Uploaded files to document library, Uploaded file changes to document library.

7. Site permissions activities: Added site collection admin, Added user of group to Cloud-based Enterprise Storage group, Broke permission level inheritance, Broke sharing inheritance, Created group, Deleted group, Modified access request setting, Modified “Members Can Share” setting, Modified permission level on site collection, Modified site permissions, Removed site collection admin, Removed permission level from site collection, Removed user or group from Cloud-based Enterprise Storage group, Requested site admin permissions, Restored sharing inheritance, Updated group.
8. Site administration activities: Added allowed data location, Added exempt user agent, Added geo location admin, Allowed user to create groups, Cancelled site geo move, Changed a sharing policy, Changed deice access policy, Changed exempt user agents, Changed network access policy, Completed site geo move, Created Sent To connection, Created site collection, Deleted orphaned hub site, Deleted Sent To connection, Deleted site, Enabled document preview, Enabled legacy workflow, Enabled Office on Demand, Enabled result source for People Searched, Enabled RSS feeds, Failed site swap, Joined site to hub site, Registered hub site, Removed allowed data location, Removed geo location admin, Renamed site, Scheduled site rename, Scheduled site swap, Scheduled site geo move, Set host site, Set storage quota for geo location, Swapped site, Unjoined site from hub site, Unregistered hub site.
9. Cloud-based Email Server mailbox activities: Created mailbox item, Copied messages to another folder, User signed in to mailbox, Accessed mailbox items, Sent message using Send On Behalf permissions, Purged messages from mailbox, Moved messages to Deleted Items folder, Moved messages to another folder, Sent message using Send As permissions, Sent message, Updated message, Deleted messages from Deleted Items folder, New-Inbox Rule Create-Inbox Rule from email web application, Set-Inbox Rule Modify inbox rule from email web application, Update inbox rules from email web application, Added delegate mailbox permissions, Removed delegate mailbox permissions, Added permissions to folder, Modified

permissions of folder, Removed permissions from folder, Added or removed user with delegate access to calendar folder, Labeled message as a record.

10. Retention policy and retention level activities: Created retention label, Created retention policy, Configured settings for a retention policy, Deleted retention label, Deleted retention policy, Deleted settings from a retention policy, Updated retention label, Updated retention policy, Updated settings for a retention policy, Enabled regulatory record option for retention labels.
11. User administration activities: Added user, Deleted user, Set license properties, Reset user password, Changed user password, Changed user license, Updated user, Set property that forces user to change password, Organization Signup, Organization Creation, User creation without organization, Password reset requested, Disable user, Login success, Login success reauthenticate, Login failure, Login failure reauthentication, Logout, User permission change, Role permission change, Environment permissions change, Create role, Edit role - add user, Edit role - remove user, Edit role - change external group mapping, Delete role.
12. Enterprise User Administration group administration activities: Added group, Updated group, Deleted group, Added member to group, Removed member from group.
13. Application administration activities: Added service principal, Removed a service principal from the directory, Set delegation entry, Removed credentials from a service principal, Added delegation entry, Added credentials to a service principal, Removed delegation entry.
14. Role administration activities: Added member to Role, Removed a user from a directory role, Set company contact information.
15. Directory administration activities: Added a partner to the directory, Removed a partner from the directory, Added domain to company, Removed domain from company, Updated domain, Set domain authentication, Verified domain, Updated the federation settings for a domain, Verified email verified domain, Turned on Enterprise

Information Technology Account Administration sync, Set password policy, Set company information.

16. eDiscovery activities: Created content search, Deleted content search, Changed content search, Started content search, Stopped content search, Started export of content search, Started export report, Previewed results of content search, Purged results of content search, Started analysis of content search, Removed export of content search, Removed preview results of content search, Removed purse action performed on content search, Removed analysis of content search, Removed search report, Content search preview item listed, Content search preview item viewed, Content search preview item downloaded, Downloaded export of content search, Created search permissions filter, Deleted search permissions filter, Changed search permissions filter, Created hold in eDiscovery case, Deleted hold in eDiscovery case, Changed hold in eDiscovery case, Created eDiscovery case, Deleted hold in eDiscovery case, Changed hold in eDiscovery case, Created eDiscovery case, Deleted eDiscovery data, Changed hold in eDiscovery case, Added member to eDiscovery case, Removed member from eDiscovery case, Changed eDiscovery case membership, Created eDiscovery administrator, Deleted eDiscovery administrator, Changed eDiscovery administrator membership, Remediation action created, Item deleted using Remediation, Created workingset search, Updated workingset search, Deleted workingset search, Previewed workingset search, Document viewed, Document annotated, Document downloaded, Tag created, Tag edited, Tag deleted, Tag files, Tag job, Created review set, Added Cloud-based productivity software data, Added non-office data, Added data to another workingset, Added remediated data, Run algo job, Run export job, Run burn job, Run error remediation job, Run load comparison job, Updated case settings.
17. eDiscovery system command activities: Created content search, Deleted content search, Changed content search, Started content search, Stopped content search, created content search action, Deleted content search action, Created search

permissions filter, Deleted search permissions filter, Changed search permissions filter, Created hold in eDiscovery case, Deleted hold in eDiscovery case, Changed hold in eDiscovery case, Created search query for eDiscovery case hold, Deleted search query for eDiscovery case hold, Changed search query for eDiscovery case hold, Created eDiscovery case, Deleted eDiscovery case, Changed eDiscovery case, Added member to eDiscovery case, Removed member from eDiscovery case, Changed eDiscovery case membership, Created eDiscovery administrator, Deleted eDiscovery administrator, Changed eDiscovery administrator membership.

18. Data Analysis application activities: Viewed program dashboard, Created program dashboard, Edited program dashboard, Deleted program dashboard, Shared program dashboard, Printed program dashboard, Copied program dashboard, Viewed program tile, Exported program tile data, Viewed program report, Deleted program report, Printed program report page, Created program report, Edited program report, Copied program report, Exported program artifact to another file format, Export program activity events, Updated program workspace access, Restored program workspace, Updated program workspace, Viewed program metadata, Created program dataset, Deleted program dataset, Created program group, Deleted program group, Added program group members, Retrieved program groups, Retrieved program dashboard, Retrieved data sources from program dataset, Retrieved upstream data flows from program dataflow, Retrieved data sources from program dataflow, Removed program group members, Retrieved links between datasets and dataflows, Created organizational program content pack, Created program app, Installed program app, Updated program app, Updated organization’s program settings, Started program trial, Started program extended trial, Analyzed program dataset, Created program gateway, Deleted program gateway, Added data source to program gateway, Removed data source from program gateway, Changed program gateway admins, Changed program gateway data source users, Set scheduled refresh on program dataset, Unpublished program

app, Deleted organizational program content pack, Renamed program dashboard, Edited program dataset, Updated capacity display name, Changed capacity state, Updated capacity admin, Changed capacity user assignment, Migrated workspace to a capacity, Removed workspace from a capacity, Retrieved program workspaces, Shared program report, Generated program Embed Token, Discover program dataset data sources, Updated program dataset data sources, Requested program dataset refresh, Binded program dataset to gateway, Changed program dataset data sources, Requested program dataset refresh, Binded program dataset to gateway, Changed program dataset connections, Took over program dataset, Updated program gateway data source credentials, Imported file to program, Updated program dataset parameters, Generated program dataflow SAS token, Created program dataflow, Updated program dataflow, Deleted program dataflow, Viewed program dataflow, Exported program dataflow, Set scheduled refresh on program dataflow, Requested program dataflow refresh, Received program dataflow secret from Key Vault, Attached dataflow storage account, Migrated dataflow storage location, Updated dataflow storage assignment permissions, Set dataflow storage location for workspace, Took ownership of program dataflow, Canceled program dataflow refresh, Created program email subscription, Updated program email subscription, Deleted program email subscription, Created program folder, Deleted program folder, Updated program folder, Added program folder access, Deleted program folder access, Updated program folder access, Posted program comment, Deleted program comment, Analyzed program report, Viewed program usage metrics, Edited program dataset endorsement, Edited program dataflow endorsement, Edited program report endorsement, Edited program app endorsement, Retrieved list of modified workspaces in program tenant, Sent a scan request in program tenant, Retrieve scan result in program tenant, Inserted snapshot for user in program tenant, Updated snapshot for user in program tenant, Deleted snapshot for user in program tenant, Inserted snapshot for user in program tenant,

Updated snapshot for user in program tenant, Deleted snapshot for user in program tenant, Retrieved snapshots for user in program tenant, Edited program certification permission, Took over a program data source, Updated capacity custom settings, Created workspace for program template app, Deleted workspace for program template app, Updated settings for program template app, Updated testing permissions for program template app, Created program template app, Deleted program template app, Promoted program template app, Installed program template app, Updated parameters for installed program template app, Created install ticker for installing program template app, Updated an organizational custom visual, Created an organizational custom visual, Deleted an organizational custom visual, Custom visual requested Enterprise Information Technology Account Administration access token, Customer visual requested Cloud-based productivity software access token, Connected to program dataset from external app, Created program dataset from external app, Deleted program dataset from external app, Edited program dataset from external app, Requested program dataset refresh from external app, Requested SAS token for program storage, Requested account key for program storage, Assigned a workspace to a deployment pipeline, Removed a workspace from a deployment pipeline, Deleted deployment pipeline, Created deployment pipeline, Deployed to a pipeline stage, Updated deployment pipeline configuration, Updated deployment pipeline access, Added external resource, Added link to external resource, Deleted link to external resource, Updated featured tables, Applied sensitivity label to program artifact, Changed sensitivity label for program artifact, Deleted sensitivity label from program artifact.

19. Productivity Analysis activities: Updated privacy setting, Updated data access setting, Uploaded organization data, Created meeting exclusion, Updated preferred meeting exclusion, Execute query, Canceled query, Deleted result, Downloaded report, Accessed Odata link, Viewed query visualization, Viewed explore, Created partition, Updated partition, Deleted partition, User logged in, User logged out.

20. Briefing email activities: Updated user privacy settings, Updated organization privacy settings.
21. Cloud-based Collaboration Application activities: Created team, Deleted team, Added channel, Deleted channel, Changed organization setting, Changed team setting, Changed channel setting, User signed in to Cloud-based Collaboration Application, Added members, Changed role of members, Removed members, Added bot to team, Removed bot from team, Added tab, Removed tab, Updated tab, Added connector, Removed connector, Updated connector, Downloaded analytics report, Upgraded Cloud-based Collaboration Application device, Blocked Cloud-based Collaboration Application device, Unblocked Cloud-based Collaboration Application device, Changed configuration of Cloud-based Collaboration Application device, Enrolled Cloud-based Collaboration Application device, Installed app, Upgraded app, Uninstalled app, Published app, Updated app, Deleted app, Deleted all organization apps, Performed action on card, Added scheduling group, Edited scheduling group, Deleted scheduling group, Added shift, Edited shift, Deleted shift, Added time off, Edited time off, Deleted time off, Added open shift, Edited open shift, Deleted open shift, Shared schedule, Clocked in using Time clock, Clocked out using Time clock, Started break using Time clock, Ended break using Time clock, Added Time clock entry, Edited Time clock entry, Deleted Time clock entry, Added shift request, Responded to shift request, Canceled shift request, Changed schedule setting, Added workforce integration, Accepted off shift message.
22. Cloud-based Collaboration Application approvals activities: Created new approval request, Viewed approval request details, Approved approval request, Rejected approval request, Canceled approval request, Shared approval request, File attached to approval request, Reassigned approval request, Added e-signature to approval request.
23. Enterprise Social Network activities: Changed data retention policy, Changed network configuration, Changed network profile settings, Changed private content

mode, Changed security configuration, Created file, Created group, Deleted group, Deleted message, Downloaded file, Exported data, Shared file, Suspended network user, Suspended user, Updated file description, Updated file name, Viewed file.

24. Enterprise Customer Relationship Management activities: Accessed out-of-box entity (deprecated), Accessed custom entity (deprecated), Accessed admin entity (deprecated), Performed bulk actions (deprecated), All Enterprise Customer Relationship Management activities, Accessed Enterprise Customer Relationship Management admin center (deprecated), Accessed internal management tool (deprecated), Signed in or out (deprecated), Activated process or plug-in (deprecated).
25. Information Systems Infrastructure Automation activities: Created flow, Edited flow, Deleted flow, Edited flow permissions, Deleted flow permissions, Started a Flow paid trial, Renewed a Flow paid trial.
26. Application authoring program activities: Created app, Edited app, Deleted app, Launched app, Published app, Marked app as Hero, Marked app as Featured, Edited app permission, Restored app version.
27. Enterprise Automation DLP activities: Created DLP Policy, Updated DLP Policy, Deleted DLP Policy.
28. Video platform activities: Created video, Edited video, Deleted video, Uploaded video, Downloaded video, Edited video permission, Viewed video, Shared video, Liked video, Unliked video, Commented on video, Deleted video comment, Uploaded video text track, Deleted video text track, Uploaded video thumbnail, Deleted video thumbnail, Replaced video permissions and channel links, Marked video public, Marked video private, Created Video platform group, Edited Video platform group, Deleted Video platform group, Edited Video platform group memberships, Created Video platform channel, Edited Video platform channel, Deleted a Video platform channel, Replaced Video platform channel thumbnails, Edited Video platform user settings, Edited tenant settings, Edited global role members, Deleted Video platform

user, Deleted Video platform user's data report, Edited Video platform user, Exported Video platform user's data report, Downloaded Video platform user's data report, Video Platform Event Date, Video Platform Event Name, Video Platform Event Description, Video Platform Meeting Code, Video Platform Participant Identifiers.

29. Content explorer activities: Accessed item
30. Quarantine activities: Previewed Quarantine message, Deleted Quarantine message, Released Quarantine message, Exported Quarantine message, Viewed Quarantine Message's header.
31. Customer Key Service Encryption activities: Fallback to Availability Key
32. Form application activities: Created form, Edited form, Moved form, Deleted form, Viewed form, Previewed form, Exported form, Allowed share form for copy, Added form co-author, Removed form co-author, Viewed response page, Created response, Updated response, Deleted all responses, Deleted response, Viewed responses, Viewed response, Created summary link, Deleted summary link, Updated from phishing status, Updated user phishing status, Sent premium form product invitation, Updated form setting, Updated user setting, Listed forms.
33. Sensitivity label activities: Applied sensitivity label to site, Removed sensitivity label from site, Applied sensitivity label to file, Changed sensitivity label applied to file, Removed sensitivity label from file.
34. Local machine communications platform system command activities: Set tenant federation.
35. Search activities: Performed email search, Performed Cloud-based Enterprise Storage search.
36. Security analytics activities: Attempted to compromise accounts.
37. Device activities: Printed file, Deleted file, Renamed file, Created file, Modified file, Read file, Captured screen, Copied file to removable media, Copied file to network share, Copied file to clipboard, Uploaded file to cloud, File accessed by an unallowed application.

38. Information barrier activities: Removed segment from site, Changed segment of site, Applied segment to site.
39. On-premises DLP scanning activities: Matched DLP rule, Enforced DLP rule.
40. Individual Productivity Analytics activities: Updated user settings, Updated organization settings.
41. Exact Data Match (EDM) activities: Created EDM schema, Modified EDM schema, Removed EDM scheme, Completed EDM data upload, Failed EDM data upload.
42. Enterprise Information System Information Protection activities: Accessed file, Discovered file, Applied sensitivity label, Updated sensitivity label, Removed sensitivity label, Removed file, Applied protection, Changed protection, Removed protection, Received AIP heartbeat.
43. Data Repository Team Discussion Post Actions: Team Discussion Post Updated, Team Discussion Post Destroyed.
44. Data Repository Team Discussion Post Reply Actions: Team Discussion Post Reply Updated, Team Discussion Post Reply Destroyed.
45. Data Repository Enterprise Actions: Self-Hosted Runner Removed, Self-Hosted Runner Registered, Self-Hosted Runner Group Created, Self-Hosted Runner Group Removed, Self-Hosted Runner Removed From Group, Self-Hosted Runner Added To Group, Self-Hosted Runner Group Member List Updated, Self-Hosted Runner Group Configuration Changed, Self-Hosted Runner Updated.
46. Data Repository Hook Actions: Hook Created, Hook Configuration Changed, Hook Destroyed, Hook Events Altered.
47. Data Repository Integration Installation Request Actions: Integration Installation Request Created, Integration Installation Request Closed.
48. Data Repository Issue Action: Issue Destroyed.
49. Data Repository Org Actions: Secret Action Created, Member Creation Disabled, Two Factor Authentication Requirement Disabled, Member Creation Enabled, Two Factor Authentication Enabled, Member Invited, Self-Hosted Runner Registered,

Secret Action Removed, Member Removed, Outside Collaborator Removed, Self-Hosted Runner Removed, Self-Hosted Runner Group Created, Self-Hosted Runner Group Removed, Self-Hosted Runner Group Updated, Secret Action Updated, Repository Default Branch Named Updated, Default Repository Permission Updated, Member Role Updated, Member Repository Creation Permission Updated.

50. Data Repository Organization Label Actions: Default Label Created, Default Label Updated, Default Label Destroyed.
51. Data Repository Oauth Application Actions: Oauth Application Created, Oauth Application Destroyed, Oauth Application Secret Restet, Oauth Application Token Revoked, Oauth Application Transferred.
52. Data Repository Profile Picture Actions: Organization Profile Picture Updated.
53. Data Repository Project Actions: Project Board Created, Project Board Linked, Project Board Renamed, Project Board Updated, Project Board Deleted, Project Board Unlinked, Project Board Permissions Updated, Project Board Team Permissions Updated, Project Board User Permission Updated.
54. Data Repository Protected Branch Actions: Branch Protection Enabled, Branch Protection Destroyed, Branch Protection Enforced For Administrators, Branch Enforcement Of Required Code Owner Enforced, Stale Pull Request Dismissal Enforced, Branch Commit Signing Updated, Pull Request Review Updated, Required Status Check Updated, Requirement For Branch To Be Up To Date Before Merging Changed, Branch Update Attempt Rejected, Branch Protection Requirement Overridden, Force Push Enabled, Force Push Disabled, Branch Deletion Enabled, Branch Deletion Disabled, Linear Commit History Enabled, Linear Commit History Disabled.
55. Data Repository Repo Actions: User Visibility Changed, Actions Enabled For Repository, Collaboration Member Added, Topic Added To Repository, Repository Archived, Anonymous Git Read Access Disabled, Anonymous Git Read Access Enabled, Anonymous Git Read Access Setting Locked, Anonymous Git Read

Access Setting Unlocked, New Repository Created, Secret Created For Repository, Repository Deleted, Repository Enabled, Secret Removed, User Removed, Self-Hosted Runner Registered, Topic Removed From Repository, Repository Renamed, Self-Hosted Runner Updated, Repository Transferred, Repository Transfer Started, Repository Unarchived, Secret Action Updated.

56. Data Repository Dependency Graph Actions: Dependency Graph Disabled, Dependency Graph Disabled For New Repository, Dependency Graph Enabled, Dependency Graph Enabled For New Repository.
57. Data Repository Secret Scanning Actions: Secret Scanning Disabled For Individual Repository, Secret Scanning Disabled For All Repositories, Secret Scanning Disabled For New Repositories, Secret Scanning Enabled For Individual Repository, Secret Scanning Enabled For All Repositories, Secret Scanning Enabled For New Repositories.
58. Data Repository Vulnerability Alert Actions: Vulnerable Dependency Alert Created, Vulnerable Dependency Alert Dismissed, Vulnerable Dependency Alert Resolved.
59. Data Repository Team Actions: Member Added To Team, Repository Added To Team, Team Parent Changed, Team Privacy Level Changed, Team Created, Member Demoted In Team, Team Destroyed, Member Promoted In Team, Member Removed From Team, Repository Removed From Team.
60. Data Repository Team Discussion Actions: Team Discussion Disabled, Team Discussion Enabled.
61. Data Repository Workflow Actions: Workflow Run Cancelled, Workflow Run Completed, Workflow Run Created, Workflow Run Deleted, Workflow Run Rerun, Workflow Job Prepared.
62. Data Repository Account Actions: Billing Plan Change, Plan Change, Pending Plan Change, Pending Subscription Change.
63. Data Repository Advisory Credit Actions: Accept Credit, Create Credit, Decline Credit, Destroy Credit.

64. Data Repository Billing Actions: Change Billing Type, Change Email.
65. Data Repository Bot Alerts Actions: Disable Bot, Enable Bot.
66. Data Repository Bot Alerts for New Repository Actions: Disable Alerts, Enable Alerts.
67. Data Repository Bot Security Alerts for Update Actions: Disable Security Update Alerts, Enable Security Update Alerts.
68. Data Repository Bot Security Alerts for New Repository Actions: Disable New Repository Security Alerts, Enable New Repository Security Alerts.
69. Data Repository Environment Actions: Create Actions Secret, Delete, Remove Actions Secret, Update Actions Secret.
70. Data Repository Git Actions: Clone, Fetch, Push.
71. Data Repository Marketplace Agreement Signature Actions: Create.
72. Data Repository Marketplace Listing Actions: Approve, Create, Delist, Redraft, Reject
73. Data Repository Members Can Create Pages Actions: Enable, Disable
74. Data Repository Organization Credential Authorization Actions: Security Assertion Markup Language Single-Sign On Authorized, Security Assertion Markup Language Single-Sign On Deauthorized, Authorized Credentials Revoked.
75. Data Repository Package Actions: Package Version Published, Package Version Deleted, Package Deleted, Package Version Restored, Package Restored.
76. Data Repository Payment Method Actions: Payment Method Cleared, Payment Method Created, Payment Method Updated.
77. Data Repository Advisory Actions: Security Advisory Closed, Common Vulnerabilities And Exposures Advisory Requested, Data Repository Security Advisory Made Public, Data Repository Security Advisory Withdrawn, Security Advisory Opened, Security Advisory Published, Security Advisory Reopened, Security Advisory Updated.

78. Data Repository Content Analysis: Data Use Settings Enabled, Data Use Settings Disabled.
79. Data Repository Sponsors Actions: Repo Funding Link Button Toggle, Repo Funding Links File Action, Sponsor Sponsorship Cancelled, Sponsor Sponsorship Created, Sponsor Sponsorship Preference Changed, Sponsor Sponsorship Tier Changed, Sponsored Developer Approved, Sponsored Developer Created, Sponsored Developer Profile Updated, Sponsored Developer Request Submitted For Approval, Sponsored Developer Tier Description Updated, Sponsored Developer Newsletter Sent, Sponsored Developer Invited From Waitlist, Sponsored Developer Joined From Waitlist.
80. Administrator audit log events: Admin privileges grant, Group events, Marketplace login audit change, Auto provisioning automatically disabled.
81. Group enterprise audit log events: Add service account permission, Remove service account permission, Add user, Add user role, Remove user, Request to join, Approve join request, Reject join request, Invite user, Accept invitation, Reject invitation, Revoke invitation, Join, Ban user including with moderation, Unban user, Add all users in domain, Create group, Delete group, Create namespace, Delete namespace, Change info setting, Add info setting, Remove info setting, Add member role, Remove user role, Membership expiration added, Membership expiration removed, Membership expiration updated.
82. Software vendor employee interaction events: Event date, Software product name, Software vendor employee email, Software vendor employee home office location, Software vendor employee access justification, Justification tickets, Log ID, Software product resource accessed name.
83. Login events: Two-step verification enabled, Two-step verification disabled, Account password change, Account recovery email change, Account recovery phone change, Account recovery secret question change, Account recovery secret answer change, Advanced Protection enroll, Advanced Protection unenroll, Failed login, Government-

backed attack attempt, Leaked password detected, Login challenged, Login verification, Logout, Out of domain email forwarding enabled, Successful login, Suspicious Login, Suspicious login blocked, Suspicious login from less secure app blocked, Suspicious programmatic login locked, User suspended, User suspended through spam relay, User suspended through spam, User suspended through suspicious activity.

84. OAuth Token audit log events: OAuth event description, OAuth event name, OAuth user, OAuth application name, OAuth client ID, OAuth scope, OAuth event data, OAuth logged activity IP address.
85. Rules audit log events: Rule event name, Rule event description, Rule triggering user, Rule name, Rule type, Rule resource name, Resource ID, Resource title, Resource type, Resource owner, Recipients, Data source, Actor IP address, Rule severity, Scan type, Matched trigger, Matched detectors, Triggered actions, Suppressed actions, Date, Device ID, Device type.
86. SAML audit log events: SAML event description, SAML Event name, SAML triggering user, SAML application name, SAML user organization name, Initiated by, Failure type, Response status, Second level status, SAML logged activity IP address, SAML event date.
87. Calendar application audit log events: Activity name, Activity description, Calendar user, Calendar ID, Event title, Event ID, User agent, Recipient email, Message ID, Remote Exchange Web Server URL, Error code, Requested window start, Requested window end, Date, Calendar logged activity IP address.
88. Context-Aware Access audit log events: Event name, Context-Aware access user, Context-Aware access logged activity IP address, Device ID, Access level applied, Context-Aware access event date.
89. Web browser audit log events: Web browser event name, Web browser event date, Web browser event reason, Device name, Device user, Web browser profile user name, URL generating event, Operating System of Web Browser, Web browser

triggered rule reason, Web browser event result, Web browser content name, Web browser content size, Web browser content hash, Web browser content type, Web browser trigger type, Web browser trigger user, Web browser user agent, Web browser client type.

90. Data Visualization audit log events: Asset name, Event description, User, Event name, Date, Asset type, Owner, Asset ID, IP address, Connector type, visibility, Prior visibility.
91. Devices audit log events: Device ID, Event description, Date, Event name, User, Device type, Application hash, Serial number, Device model, OS version, Policy name, Policy status code, Windows OS edition, Account registration change, Device action event, Device application change, Device compliance status, Device compromise, Device OS update, Device ownership, Device settings change, Device status changed on Apple portal, Device sync, Failed screen unlock attempts, Sign out user, Suspicious activity, Work profile support.
92. Cloud-based web storage application audit log events: Cloud-based web storage application event name, Cloud-based web storage application event description, Cloud-based web storage application item type, Cloud-based web storage application item ID, Cloud-based web storage application item visibility, Cloud-based web storage application item prior visibility, Cloud-based web storage application user, Cloud-based web storage application visitor Boolean value, Cloud-based web storage application file owner, Cloud-based web storage application event date, Cloud-based web storage application event IP address
93. Groups audit log events: Groups event name, Groups event description, Groups event user, Groups event date.
94. Chat audit log events: Chat event name, Chat event description, Chat event user, Chat event date.

95. Whiteboard application audit log events: Whiteboard application ID Whiteboard application event description, Whiteboard application event name, Whiteboard application event user, Whiteboard application event date.
96. Note application audit log events: Note application event name, Note application event description, Note application event user, Note application event note owner, Note application event date, Note application note URI, Note application attachment URI.
97. Password vault audit log events: Password vault actor, Password vault event timestamp, Password vault event name, Password vault application username, Password vault application installation name, Password vault application credential name.
98. Takeout audit log events: Takeout event description, Takeout products requested, Takeout Job ID, Takeout event date, Takeout event IP address.
99. User accounts audit log events: User account event description, User account event date, User account event IP address, two-step verification disable, two-step verification enroll, Account password change, Account recovery email change, Account recovery phone change, Account recovery secret question change, Account recovery secret answer change.
100. Voice audit log events: Voice event name, Voice event description, Voice event date, Voice event user, Voice receiving phone number, Voice placing phone number, Voice call duration, Voice group message status, Voice call cost, Auto Attendant couldn't route to voicemail recipient, Auto attendant deleted, Auto attendant failed to transfer to a user, Auto attendant published, Auto attendant received a voicemail, Auto attendant voicemail failed to deliver, Auto attendant voicemail failed to forward.
101. User setting changes: 2-Step Verification Scratch Codes Of User Deleted, New 2-Step Verification Scratch Codes Generated For User, 3-Legged Oauth Device Tokens Revoked, 3-Legged Oauth Token Revoked, Add Recovery Email For User, Add Recovery Phone For User, Admin Privileges Granted For User, Admin

Privileges Revoked For User, Application Specific Password Revoked For User, Automatic Contact Sharing Changed For User, Bulk Upload Notification, User Invite Cancelled, Custom Attribute Changed, External Id Changed, Gender Changed, Ims Changed, IP Whitelisted, Keywords Changed, User Location Changed, User Organization Changed, User Phone Numbers Changed, User Recovery Email Changed, User Recovery Phone Changed, User Relation Changed, User Address Changed, User Email Monitor Created, Data Transfer Requested For User, Delegated Admin Privileges Granted, Account Information Dump Deleted, Email Monitor Deleted, Mailbox Dump Deleted, Profile Photo Deleted, First Name Changed, Gmail Account Reset, Last Name Changed, Mail Routing Destination Created, Mail Routing Destination Deleted, Nickname Created, Nickname Deleted, Password Changed, Password Change Required On Next Login, Recovery Email Removed, Recovery Phone Removed, Account Information Requested, Mailbox Dump Requested, User Invite Resent, Cookies  Reset For User And Forced Relogin, Security Key Registered For User, Security Key Revoked, User Invite Sent, Temporary Password Viewed, 2-Step Verification Turned Off, User Session Unblocked, Profile Photo Updated, User Advanced Protection Unenroll, User Archived, User Birthdate Changed, User Created, User Deleted, User Downgraded From Social Media Application, User Enrolled In 2-Step Verification, User List Downloaded, User Org Unit Changed, User Put In 2-Step Verification Grace Period, User Renamed, User Strong Auth Unenrolled, User Suspended, User Unarchived, User Undeleted, User Unsuspended, User Upgraded To Social Media Application.

102. Application Authoring application audit log elements: App synced, App edited, App added, App deleted, App invocation added, App invocation edited, App invocation deleted, App invocation action performed, App read call made, App bot invocation.
103. Organizational Administrative Data Elements: Set Terms and Conditions, Modify Terms and Conditions, Set org custom theme, Edit org custom theme, Add custom policy, Delete custom policy, Create User IdP Profile, Create environment, Delete

environment, Rename environment, Edit domain name, Create business group, Edit business group name, Edit business group entitlement, Delete business group.

104. API audit log elements: Create API, Delete API, Import API, Update label of API, Update consumer endpoint of API, Update endpoint URI of API, Calendar API kind, Application API client version, Create API version, Delete API version, Import API, Edit name of API version, Edit description of API version, Edit API URL of API version, Add tag to API, Remove tag from API, Deprecate API, Set T&Cs, Create RAML, Modify RAML, Create endpoint, Update existing endpoint, Deploy proxy, Update deployed proxy, Redeploy proxy, Create SLA tier, Modify SLA tier, Deprecate SLA tier, Delete SLA tier, Apply policy, Edit policy, Remove policy, Create project, Delete project, Delete files, Rename project, Clean branch, Create branch, Delete branch, Save branch, Delete file, Move file, Import project, Publish to **Exchange**, Publish to API Platform, Add dependencies, Remove dependencies, Change dependencies, Reload dependencies, Merge Branch, Share project, Sync with **Data Repository**, Unsync with **Data Repository**, Modify organization settings, Rename branch, Modify project settings.
105. API Metadata: Create an API instance, Delete an API instance, Update an API instance
106. Application Data: Create application, Delete application, Reset client secret, Request access, Request tier change, Request tier change approval, Approve application, Revoke application, Restore application, Create Mocking Service link, Delete Mocking Service link, Create/modify/delete Object store, Upload file, Delete file, Update file
107. Private Portals audit log events: Create portal, Modify portal association, Delete portal, Add portal page, Make portal page visible, Delete portal page, Edit portal page, Hide portal page, Set portal theme, Modify portal theme, Modify portal security, Create a page, Update a page, Delete a page, Publish a portal.

108. Public Portals audit log events: Update a domain, Delete a domain, Create a page, Delete a page, Update a page, Create a portal, Publish a portal, Delete a portal, Update a portal
109. Identity Management audit log events: Create identity provider configuration, Edit identity provider configuration, Delete identity provider configuration, Warning, Create identity management key, Set primary identity management key, Delete identity management key
110. Connected App audit log events: Create Connected Application, Edit Connected Application, Delete Connected Application, Update Scope Assignments, Application Authorization Approved, Application Authorization Denied, Token Retrieval Success, Token Retrieval Failed, Revoke Access/Refresh Tokens
111. Team audit log events: Create Team, Update Team, Move Team, Add Members, Remove Members, Add Permissions, Remove Permissions, Edit External Group Mappings, Delete Team
112. Asset Management audit log events: Create an asset, Update an asset, Delete an asset, Share an asset, Publish an asset to public portal, Remove an asset from public portal, Update an asset icon, Delete an asset icon, Create a managed tag (category), Delete a managed tag (category), Delete an organization, Update tags, Create a tag configuration, Update a tag configuration, Delete a tag configuration
113. Asset Review audit log events: Create a Comment, Delete a comment, Update a comment, Create a review, Delete a review, Update a review
114. Runtime Manager audit log events: Create application, Start application, Restart application, Stop application, Delete application, Change application zip file, Promote application from sandbox, Change application runtime, Change application worker size, Change application worker number, Enable/disable persistent queues, Enable/disable persistent queue encryption, Modify application properties, Enable/disable insight, Modify log levels, Create/modify/delete alerts, Enable/disable alerts, Create/modify/delete application data, Create/modify schedules,

Create/modify/delete tenants, Enable/disable schedules, Clear queues, Enable/Disable static IP, Allocate/release static IP, LoadBalancer Create/modify/delete, Create/modify/delete alerts V2, Create/modify/delete VPC, Create/modify/delete VPN

115. Server audit log events: Add server, Delete server, Rename server, Create server group, Delete server group, Rename server group, Add server to server group, Remove server from server group, Create cluster, Delete Cluster, Rename cluster, Add server to cluster, Remove server from cluster, Deploy application, Delete application, Start application, Stop application, Redeploy application with existing file, Redeploy application with new file.
116. Private Spaces audit log events: Create/Modify/Delete private space, Create/Modify/Delete connection, Create/Modify/Delete VPN, Create/Modify/Delete transit gateway, Create/Modify/Delete TLSContext, Create/Modify/Delete routes
117. Anypoint MQ audit log events: Create/modify/delete/purge queue, Create/modify/delete exchange, Create/delete exchange binding, Create/delete/regenerate client

**RECORD SOURCE CATEGORIES:**

Employees; contractors; customers.

**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.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Automated database, computer storage media, and paper.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records relating to system administration are retrievable by user ID.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Records relating to system administration 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.

**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 Chief Information Officer and Executive Vice President and include their name and address.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

None.

**HISTORY:**

May 10th, 2021; 86 FR 24902

**SYSTEM NAME AND NUMBER:**

830.000 Customer Service and Correspondence

**SECURITY CLASSIFICATION:**

None.

**SYSTEM LOCATION:**

USPS Customer Experience, Headquarters; Integrated Business Solutions Services Centers; the National Customer Support Center (NCSC); districts, Post Offices contractor sites; and detached mailing units at customer sites

**SYSTEM MANAGER(S):**

Chief Customer and Marketing 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 enable review and response services for customer inquiries and concerns regarding USPS and its

products and services.

2. To ensure that customer accounts and needs are attended to in a timely manner.

3. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.

4. To protect USPS customers from becoming potential victims of mail fraud and identity theft.

5. To identify and mitigate potential fraud in the COA and Hold Mail processes.

6. To verify a customer's identity when applying for COA and Hold Mail services.

7. To support (or facilitate) the administration of Operation Santa, Letters to Santa, or similar programs.

8. To track employee performance and productivity through dashboard metrics and analysis.

9. To set and track employee goals relating to Customer Relationship Management Software metrics

10. To create competitions to encourage productivity and promote team effectiveness.

11. To provide business customer data to other systems through APIs

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

This system contains records relating to customers who contact customer service by online and offline channels. This includes customers making inquiries via e-mail, 1-800-ASKUSPS, other toll-free contact centers, or the Business Service Network (BSN), as well as customers with product-specific service or support issues.

This system also contains records relating to employees who utilize the dashboard analysis and productivity application.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

*1. Customer information:* Customer and key contact name, mail and e-mail address, phone and/or fax

number; customer ID(s); title, role, and employment status; company name, location, type and URL; vendor

and/or contractor information.

*2. Identity verification information:* Last four digits of Social Security Number (SSN), username and/or password, DU-N-S Number, mailer ID number, publisher ID number, security level and clearances, and business customer number.

*3. Product and/or service use information:* Product and/or service type, product numbers, technology
specifications, quantity ordered, logon and product use dates and times, case number, pickup number, article
number, and ticket number.

*4. Payment information:* Credit and/or debit card number, type, and expiration date; billing information; checks, money orders, or other payment method.

*5. Customer preferences:* Drop ship sites and media preference.

*6. Service inquiries and correspondence:* Contact history; nature of inquiry, dates and times, comments, status, resolution, and USPS personnel involved.

7. *Employee scorecard analysis:* Scorecard Metrics, Scorecard Activity Score, Scorecard Objective Score, Scorecard Smart Target, Scorecard Target, Leaderboard Standings, Competition Name, Competition Results, Formula Metrics, Formula Builder Metrics, Accolade Achievements, Goal Name, Goal Description, Goal Category, Goal Visibility, Goal Owner, Goal Category, Workflow Name, Workflow Description, Workflow Hierarchy Level, Workflow Time Group, Competitor Name, Competitor Rank, Competitor Score, Competitor Selection, Group Name, Workflow Metric, Workflow Message, Workflow Image, Workflow Entities, Workflow Action, Workflow Status, Workflow Rank, Workflow Operator, Workflow Value, Workflow Schedule, Workflow Creator, Accolade Name.

8. *Customer Relationship Management Software Metrics*: Opportunity ID, Approval Status, Stage Name, Sales Area, Sales District, Sales Title, Opportunity Owner, Owner Alias, Created Date, Current Stage Entry Date, Opportunity Name, Actual Start Date, Opportunistic Strategy, Product Group, Product Category, Account, Expected State, Lead Source, Lead Source Type, Created By, Amount Year-to-date, User Area, User District, Amount, Account Name, Opportunity Name, Lead Source Category, Age of Opportunity, Company Overview, Business Need, Solution, Results, Point of Entry Area, Point of Entry City State, Alias, Full Name, Title, Year-to-date Revenue, Tear-to-date

Target, Over/Under Target, Percentage Over/Under Target, Year-to-date Supply, Over/Under Year-to-date Supply, Percentage Over/Under Year-to-date Supply, Current Quarter to Date Sales Revenue, Current Entire Quarter Target, Remain to Quarter Target, Percentage Over/Under Quarter Target, EAS Level, Number Closed Sales Pending Sales Representative Submission, Number Closed Sales Pending Management Approval, Update Status Message, Company ID, User ID, Service, Action, Service Access ID, Service Response, Account Street, Account City, Account State, Account ZIP Code, Region, Report District, Number of Sales, Dollar Amount, Report Area, Report Title, Registration Match, Product Category, Actual Mailing, Actual Shipping, Actual Total, Interaction Type, Number of Calls, Average Talk Time, Longest Call, Resource Name, Rowlev, Interaction ID, Start Time, End Time,  Representative, Call Info, Technical Result, Incoming Phone Number, Sort, Call Type, Start Est, End Est, Status, Result Reason, Talk Time, Est Logout, Est Playback Duration, Customer Relationship Software Link, Priority Mail Number of Sales, Priority Mail Dollar Amount, Parcel/Package Number of Sales, Parcel/Packages Dollar Amount, First Class Mail Number of Sales, First Class Mail Dollar Amount, Closed Sales Area, Closed Sales District, Pricing Category, Contract Status, New Sale, Opportunity Record Type, VP Group, Lead Owner, Days Since Lead was Created, Lead ID Link, Days Owned, Lead Age, Lead Contact, Region/Team, Total Phone Calls, Total In-Person Visits, Total Video Conferences with Customer, Total Emails, Number of Active Reps with Activity, Average Phone Calls Per Rep, Average In-Person Visits Per Rep, Average Video Conferences with Customer, Average Emails Per Rep, Assigned to Area, Assigned to District, Type 2, Task/Event Record, Related To, Subject, Priority, Task, Assignee, Assigned Alias, Description, Seller’s Name, Virtual Meetings, Appointment Scheduled Last 14 Days, Appointments Scheduled Next 14 Days, Appointments Kept, Stalled Opportunities, Funnel Health, Stage 4 Opportunity Review, Stage 5 Opportunities Not Submitted, Directed Activities Review, Coachable Moments, Action Items.

**RECORD SOURCE CATEGORIES:**

For Customer Service and Correspondence: Customers and, for call center operations, commercially available sources of names, addresses, and telephone numbers.

For Employee Dashboard Analysis: Customer Relationship Management Software

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

Standard routine uses 1. through 7., 10., and 11. apply

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Automated databases, computer storage media, and paper

**POLICIES OF PRACTICES FOR RETRIEVAL OF RECORDS:**

By customer name, customer ID(s), mail or e-mail address, phone number, customer account number, case number, article number, pickup number, last four digits of SSN, ZIP Code, other customer identifier, employee name, employee email.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

1. Customer care records for usps.com products are retained 90 days.

2. Records related to 1-800-ASK-USPS, Delivery Confirmation service, Special Services, and international call centers are retained 1 year.

3. Customer complaint letters are retained 6 months and automated complaint records are retained 3 years.

4. Business Service Network records are retained 5 years.

5. Records related to Operation Santa, Letters to Santa, or similar programs are retained 6 months after the new calendar year.

6. Other records are retained 2 years after resolution of the inquiry.

7. Records relating to Dashboard Metric Analysis are retained for 1 year.

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 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. Online data transmissions are protected by encryption.

**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 information about them is maintained in this system of records must address inquiries to the system manager in writing. Inquiries should include name, address, and other identifying information.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

None.

**HISTORY:**

December 12, 2018, *83 FR 63912*; June 27, 2012, *77 FR 38342*; April 29, 2005, *70 FR 22516*.

**Sarah Sullivan,**

*Attorney, Ethics & Legal Compliance.*

BILLING CODE P

[FR Doc. 2023-19812 Filed: 9/13/2023 8:45 am; Publication Date: 9/14/2023]