This document is scheduled to be published in the
Federal Register on 12/01/2023 and available online at
https://federalregister.gov/d/2023-26480, and on **https://govinfo.gov**

POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service®.

ACTION: Notice of modified system of records.

SUMMARY: The United States Postal Service® (USPS) is proposing to modify three General Privacy Act Systems of Records (SOR) to support the development and implementation of a voluntary mentorship program and related applications to assist participating employees in achieving their individual personal and professional goals.

DATES: These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**], unless responses 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 (privacy@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 three existing systems of records (SOR) to support the implementation of voluntary mentorship programs and related applications.

I. Background

The USPS is planning to implement voluntary mentorship programs to support professional growth and promote diversity, equity, inclusion, and accessibility, consistent with the Postal Service's Delivering for America plan. These mentorship programs will use an application process to select mentors and to match them with mentees. Mentors and mentees will also be asked to complete voluntary surveys to provide feedback on the program. In association with these mentorship programs, a new software application will also be implemented to help facilitate and maintain the mentorship program and assist mentors and mentees.

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

The Postal Service is proposing modifications to the following SORs:

USPS SOR 100.300, Employee Development and Training Records.

-One new Purpose, number 13

-One new Category of Records, number 3

-One new Retention and Disposal period, number 5

-One new Category of Individuals

-One new Notification Procedure

USPS SOR 550.100, Commercial Information Technology Resources-Applications.

-One new Purpose, number 12

-Three new Categories of Records, numbers 12 – 14

-One new Retention and Disposal period, number 12

-One new Retrievability process, number 12

USPS SOR 550.200, Commercial Information Technology Resources-Administrative

-One new Category of Records, number 118.

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:

USPS 100.300 Employee Development and Training Records.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Management training centers, Integrated Business Solutions Services Centers, other USPS facilities where career development and training records are stored, USPS Law Department and contractor sites.

SYSTEM MANAGER(S):

Vice President, Human Resources, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Organization Development, United States Postal Service, 475 L'Enfant Plaza SW, Washington DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 410, 1001, 1005, and 1206.

PURPOSE(S) OF THE SYSTEM:

1. To provide managers, supervisors, and training and development professionals with decision-making information for employee career development, succession planning, training, and assignment.

2. To make and track employee job assignments, to place employees in new positions, and to assist in career planning and training in general.

3. To provide statistics for personnel and workload management.

4. To provide employees with an online platform that supports individual and career development.

5. To facilitate voluntary information sharing through an enhanced employee profile tool that highlights individual education, knowledge and experience.

6. To provide employees with convenient and flexible online learning options.

7. To create a forum that promotes a culture for participation in voluntary career development activities and opportunities.

8. To create a readily available source of information about current employee talents, skills, and abilities.

9. To communicate with and provide notification to individuals about training assignments and requirements, both prior to and after effective date of employment or placement.

10. To facilitate communication between the Postal Service and individual employees, new hires and applicants, including current and former employees.

11. To share relevant information and topics about the Postal Service with individual employees, new hires and applicants, including current and former employees.

12. To request and gather voluntary feedback from individual employees, new hires and applicants, including current and former employees.

13. To facilitate registration and participation in a voluntary mentorship program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former USPS employees, new hires and applicants.

Individual employees that voluntarily participate in USPS-sponsored mentorship programs.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Employee information: Name, Social Security Number, Employee Identification Number, phone number(s), SMS text message number, personal email address, demographic information, photograph, years of service, retirement eligibility, postal assignment information, work contact information, finance number(s), duty location, and pay location.

2. Employee development and training information: Records related to career development, work history, assessments, skills bank participation, USPS- and non-USPS-sponsored training, examinations, evaluations of training, and USPS lodging when a discrepancy report is filed against the student about unauthorized activities while occupying the room.

3. Mentorship program applicant and participant information: First and last name; current position; employing office; work telephone number(s); work email address; length of tenure with the USPS and in current position; participant role; agreement to participate; objectives, goals and/or expectations for participation; communication, meeting, and match preferences; interests/hobbies; and satisfaction survey results.

RECORD SOURCE CATEGORIES:

Employees; employees' supervisor or manager; and other systems of records.

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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, digital files, and paper files.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By employee name, Social Security Number, or Employee Identification Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Training records are retained 5 years. Training-related travel records are retained 1 year.

2. Records related to succession planning and individual development planning are retained 10 years.

3. Examination records are retained 1 year after employee separation.

4. Skills bank records are retained up to 2 years.

5. Mentorship Program participant records and satisfaction survey results will be retained for up to 2 years, after the end of the Fiscal Year program cycle.

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.

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 Procedures below and Record Access Procedures above.

NOTIFICATION PROCEDURES:

Individuals wanting to know if information about them is maintained in this system must address inquiries to the facility head where currently or last employed. Headquarters employees must submit inquiries to Corporate Personnel Management, 475 L'Enfant Plaza SW, Washington, DC 20260.

Participants in the USPS Law Department Mentorship Program must submit inquiries to USPS Law Department, 475 L’Enfant Plaza SW, Washington, DC 20260.

Inquiries must include full name, Social Security Number or Employee Identification Number, name and address of facility where last employed, and dates of USPS employment.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(j) and (k), USPS has established regulations at 39 CFR 266.9 that exempt records in this system depending on their purpose. The USPS has also claimed exemption from certain provisions of the Act for several

of its other systems of records at 39 CFR 266.9. To the extent that copies of exempted records from those other systems are incorporated into this system, the exemptions applicable to the original primary system continue to apply to the incorporated records.

HISTORY:

August 18, 2021, 86 FR 46281; July 19, 2013, 78 FR 43247; June 17, 2011, 76 FR 35483; April 29, 2005, 70 FR 22516.

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):

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.

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.

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.

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.

NOTIFICATION PROCEDURES:

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.

EXEMPTION(S) PROMULGATED FROM THIS SYSTEM:

None.

HISTORY:

May 11, 2021; 86 FR 25899; January 31, 2022; 87 FR 4957.

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

118. Mentorship program application data: Notification Logs, Notification Type, Notification Template, Status, Time sent, Email Events, General Application Data, Support Tickets, Product Usage Analytics, Product update in app notification delivery status, Application error logs, Application request logs.

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:

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.

EXEMPTION(S) PROMULGATED FROM THIS SYSTEM:

None.

HISTORY:

May 10th, 2021; 86 FR 24902

Colleen Hibbert-Kapler,

Attorney, Ethics and Compliance.

[FR Doc. 2023-26480 Filed: 11/30/2023 8:45 am; Publication Date: 12/1/2023]