Summary of Changes

Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*

Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, has been updated with *Postal Bulletin* articles through February 28, 2019, as follows:

The chapter, subchapter, part, appendix, or section...	**titled...**	**was...**	**in *Postal Bulletin* issue number...**	**with an issue date of....**
Appendix — Privacy Act System of Records				
Section E	USPS 800.000	Modified to facilitate the new Address Matching Database for the purposes of protectinTg the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes.	22514	2-28-19
Section E	USPS 800.050	Established to support the new Address Matching Database that is being implemented to facilitate the prevention of fraudulent Change of Address and Hold Mail requests through address matching across Postal Service customer systems.	22514	2-28-19
Section E	USPS 810.100	Modified to facilitate the new Address Matching Database for the purposes of protecting the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes.	22514	2-28-19
Section E	USPS 810.200	Modified to facilitate the new Address Matching Database for the purposes of protecting the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes.	22514	2-28-19
Section E	USPS 820.200	Modified to facilitate the new Address Matching Database for the purposes of protecting the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes.	22514	2-28-19
Section E	USPS 820.300	Modified to facilitate the new Address Matching Database for the purposes of protecting the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes.	22514	2-28-19

The chapter, subchapter, part, appendix, or section...	**titled...**	**was...**	**in *Postal Bulletin* issue number...**	**with an issue date of....**
Section E	USPS 830.00	Modified to Support the new Address Matching Database, which will be used to identify, prevent and mitigate fraudulent activity within the Change of Address and Hold Mail processes; as well as the Operation Santa program, a long-standing program that collects the thousands of letters to Santa the USPS receives each year and allows customers to collect and fulfill gift requests for underprivileged children.	22514	2-28-19
Section E	USPS 910.000	Modified to support the new Address Matching Database, which will be used to identify, prevent and mitigate fraudulent activity within the Change of Address and Hold Mail processes; to allow for the scanning of Government issued IDs at retail locations for the purposes of verifying identity for customers who need postal products and services; and to enhance the Postal Service's existing remote identity proofing with a Phone Validation and One-Time Passcode solution.	22514	2-28-19

UNITED STATES POSTAL SERVICE®

Guide to Privacy, the Freedom of Information Act, and Records Management

Handbook AS-353

February 2019
Transmittal Letter

A. Introduction. .Key strategies of the Postal Service's Future Ready Goals are to achieve growth by adding value for customers and to improve the workplace environment. The proper collection, use, and protection of customer and employee information are key parts of that value proposition.

B. Instructions. This handbook replaces the May 2018 edition.

C. Explanation. This handbook provides direction and guidance for Postal Service™ employees, suppliers, or other authorized users with access to Postal Service records and information resources. The handbook also provides direction and guidance for customers, employees, suppliers, or other individuals about how their information is collected, maintained, used, disclosed, and safeguarded. This version of the handbook includes updates to several Systems of Records (SORs), including the creation of a new SOR, *USPS 800.050, Address Matching for Mail Fraud Detection and Prevention*.

D. Distribution. This handbook is available online on both the USPS® intranet (*http://blue.usps.gov/cpim/*) and the FOIA page at *usps.com* (*http://www.usps.com/foia*).

E. Comments. Submit questions, comments, or suggestions about this handbook to:

THOMAS J MARSHALL
GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 6004
WASHINGTON DC 20260
PHONE: 202-268-5555

F. Effective Date. This handbook is effective February 2019.

Natalie A. Bonanno

Natalie A. Bonanno
A/Associate General Counsel and
Chief Ethics & Compliance Officer

Contents

This page intentionally left blank

This page intentionally left blank

Exhibits

This page intentionally left blank

1 Introduction

1-1 Purpose of This Handbook

Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management,* describes Postal Service™ policies and procedures governing the privacy of information relating to customers, employees, or other individuals, and the release, protection, and management of Postal Service records. The Postal Service is mandated by law, and has adopted policies, to protect the privacy of its customers, employees, individuals, and suppliers. The Postal Service is also required to make its records available to the public consistent with the Freedom of Information Act (FOIA) and good business practices.

1-2 Customer Trust and Privacy Protection

For more than two centuries, the Postal Service has maintained a brand that customers trust to protect the privacy and security of their information. As the privacy landscape evolves, the Privacy Office keeps up with developing legal and policy frameworks, new technologies, and best-in-class business models and practices. The Privacy Office has developed its customer privacy policy and procedures on a synthesis of the best business models and practices of the public and private sectors. This includes established government agency laws, regulations, and guidelines, as well as privacy principles and best practices followed by the private sector.

1-3 Handbook Application

This handbook covers the laws, policies, and procedures for all Postal Service records and information related to customers, employees, individuals, and suppliers. This handbook applies to Postal Service employees, suppliers, or other authorized users with access to Postal Service records and information resources. The policies and procedures in this handbook cover the following types of information or information systems:

- Postal Service records.
- Information related to customers, employees, other individuals, and suppliers.

- Technologies, information systems, infrastructure, applications, products, services, and other information resources associated with collecting, maintaining, using, disclosing, and safeguarding customer, employee, or other individuals' information.

1-4 Roles and Responsibilities

1-4.1 General Responsibility

All Postal Service employees, business partners and suppliers, and other authorized users are responsible for following the policies and procedures in this handbook.

1-4.2 Specific Responsibility

1-4.2.1 Officers, Managers, and Employees

All officers, business and line managers, supervisors, and other employees are responsible for implementing privacy policies as required by this handbook and their Postal Service duties. Officers and managers ensure compliance with privacy policies through organizations and information resources under their direction, and provide resources required to appropriately protect the privacy of customer, employee, or other individuals' information.

1-4.2.2 Suppliers, Business Partners, and Customers

Suppliers, business partners, and customers are responsible for the following:

a. *Suppliers and Business Partners.* All Postal Service suppliers and business partners who develop systems with or have access to information resources that contain customer, employee, or other individuals' data, or who help to develop or implement a Postal Service Web site or marketing e–mail campaign, are responsible for complying with Postal Service privacy policies and related business, security, and contracting practices.

b. *Customers.* Customers must follow the applicable procedures for privacy and FOIA.

1-4.2.3 Chief FOIA Officer

The chief FOIA officer is responsible for the following:

a. Overseeing Postal Service compliance with the FOIA.

b. Making recommendations to the postmaster general regarding the Postal Service's FOIA program.

c. Monitoring and reporting on FOIA implementation and performance for the Postal Service.

Contact the chief FOIA officer at the following address:

CHIEF FOIA OFFICER
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 10433
WASHINGTON DC 20260

1-4.2.4 Chief Privacy Officer

The chief privacy officer (CPO) is responsible for the following:

a. Developing and implementing policies, processes, and procedures for privacy, records, and FOIA.

b. Reviewing privacy impact assessments and determining information sensitivity during the business impact assessment process.

c. Advising management on strategic direction and trends.

d. Evaluating technology that impacts privacy.

e. Providing guidance on privacy and records policies.

f. Directing the activities of the Privacy Office and the Records Office, and reporting to the Consumer Advocate.

Contact the Privacy Office at the following address:

PRIVACY OFFICE
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 10433
WASHINGTON DC 20260
e-mail: *privacy@usps.gov*

1-4.2.5 Manager, Records Office

The manager of the Records Office is responsible for the following:

a. Managing the Records Office.

b. Establishing procedures and guidelines to ensure that record management practices comply with the Privacy Act and FOIA.

c. Answering questions about the policies and procedures in this handbook.

Contact the Records Office manager at the following address:

MANAGER, RECORDS OFFICE
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 5821
WASHINGTON DC 20260
Telephone: 202-268-2608

1-4.2.6 Freedom of Information Act Requester Service Centers

The FOIA Requester Service Centers (RSCs) are responsible for the following:

a. Facilitating communication between the Postal Service and FOIA requesters.

b. Providing information to requesters concerning the status of FOIA requests and information about responses to such requests.

Contact the FOIA RSCs at the following addresses:

US POSTAL SERVICE — HEADQUARTERS
MANAGER RECORDS OFFICE
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 9431
WASHINGTON, DC 20260
Fax: 202-268-5353

US POSTAL SERVICE — FIELD
USPS FOIA REQUESTER SERVICE CENTER — FIELD
ST LOUIS GENERAL LAW SERVICE CENTER
1720 MARKET STREET RM 2400
ST LOUIS, MO 63155-9948
Fax: 650-578-4956

POSTAL INSPECTION SERVICE
OFFICE OF COUNSEL
US POSTAL INSPECTION SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON, DC 20260
Fax: 202-268-4538

INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL
US POSTAL SERVICE
1735 N LYNN ST STE 10000
ARLINGTON, VA 22209
Fax: 703-248-4626

1-4.2.7 Freedom of Information Act Public Liaison

The FOIA public liaison is responsible for the following:

a. Managing the FOIA RSCs.

b. Receiving concerns of requesters about the service provided by the FOIA RSCs following an initial response.

c. Ensuring a service-oriented response to requests and FOIA-related inquiries.

d. Reporting to the chief FOIA officer on its activities.

Contact the appropriate FOIA public liaison at the address provided in section 1-4.2.6.

1-4.2.8 Freedom of Information Act Coordinator

The FOIA coordinator, which is an ad hoc position located within each Headquarters department, area office, and district office, is responsible for the following:

a. Coordinating FOIA requests referred to or received by functional or geographical area.

b. Providing procedural guidance, upon request, to records custodians.

c. Assisting the manager of the Records Office with national records management activities, such as annual reporting of local FOIA and Privacy Act activities.

1-4.2.9 Records Custodian

The records custodian is responsible for ensuring that records within his/her facilities or organizations are managed according to Postal Service policies. Vice presidents or their designees are the custodians of records maintained at Headquarters. In the field, the records custodian is the head of a Postal Service facility, such as an area, district, Post Office™, or other Postal Service installation, or designee that maintains Postal Service records. Senior medical personnel are the custodians of restricted medical records maintained within Postal Service facilities. The custodian of Employee Assistance Program records is the Postal Service counselor, a supplier, or the Public Health Service, whichever provided the services.

1-4.2.10 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office, is responsible for the following:

a. Ensuring compliance with information security policies, including the protection of information resources containing customer, employee, or other individuals' information.

b. Safeguarding and disposing of electronic records (including e-mails) that are maintained in information systems, including those that are subject to legal holds.

c. Serving as the central contact for information security issues and providing security consultations as requested.

1-4.2.11 General Counsel

The general counsel or designee is responsible for the following:

a. Deciding administrative appeals filed under the Privacy Act and Freedom of Information Act (FOIA). Appropriate legal counsel should be consulted by FOIA coordinators, records custodians, and others with legal questions about the Privacy Act or FOIA. For appeals related to records other than inspector general records, contact the general counsel at the following address:

   GENERAL COUNSEL
   US POSTAL SERVICE
   475 L'ENFANT PLZ SW RM 6004
   WASHINGTON DC 20260

b. Issuing legal hold notices for the purpose of preserving Postal Service records relating to pending or anticipated legal proceedings, investigations, or audits.

1-4.2.12 Chief Postal Inspector

The chief postal inspector of the Inspection Service is responsible for handling Privacy Act and FOIA requests for Inspection Service records. Contact the chief postal inspector at the following address:

CHIEF POSTAL INSPECTOR
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 3100
WASHINGTON DC 20260

1-4.2.13 Office of Inspector General

The inspector general is responsible for handling Privacy Act and FOIA requests and appeals for Office of Inspector General records. Contact the inspector general at the following address:

FOIA OFFICER
OFFICE OF INSPECTOR GENERAL
US POSTAL SERVICE
1735 NORTH LYNN STREET, STE 10000
ARLINGTON, VA 22209

1-5 Definitions

The types of records mentioned in this handbook are defined in section 1-5.1.

1-5.1 Record

A Postal Service record includes information relating to the Postal Service or its business recorded in any medium (e.g., a hard copy or electronic document; recording in electronic, audio, video, or photographic format; tangible item; or other material) that is created, maintained, or received by Postal Service employees, business partners, and suppliers under the custody or control of the Postal Service. A record that is of a purely personal nature is not a Postal Service record. Legal holds may apply to Postal Service records as well as personal records.

Active record — Information that is used for conducting current business.

Inactive record — Information that is not used for conducting current business, but for which the retention period has not yet expired.

Permanent record — A record determined as having sufficient historical or other value to warrant continued preservation. All other records are considered temporary and must be scheduled for disposal.

Temporary record — A record determined to have insufficient value (on the basis of current standards) to warrant its permanent preservation.

1-5.2 System of Records

A file, database, or program from which information about customers, employees, or individuals is retrieved by name or other identifier.

1-5.3 Customers

External customers of the Postal Service, including individual consumers and business customers.

1-5.4 Individual

Individual consumer, employee, or other individual.

1-5.5 Legal Hold Notice

A legal hold notice is written notification issued in connection with a pending or anticipated legal proceeding, investigation, or audit that identifies records that must be preserved for the duration of the notice.

1-5.6 Retention Period

Retention period is the authorized length of time that a record series must be kept before its disposal. The period is usually stated in terms of months or years but sometimes is expressed as contingent upon the occurrence of an event. Authorized retention periods are published in eRIMS on the Postal Service intranet.

This page intentionally left blank

2 Laws, Guidelines, and Policies

2-1 The Best of Public and Private Practices

The Postal Service is subject to the privacy protection requirements of the Privacy Act, and the document access requirements of the FOIA. The Postal Service has also developed a customer privacy policy based on federal laws and guidelines and the best practices of the private sector. The privacy statutes, guidelines, and Postal Service policies described in this section provide a comprehensive privacy-protection framework.

2-2 Mail Protections

The privacy and security of the mail are core values of the Postal Service. Information from the contents or cover of any customer's mail may not be recorded or otherwise collected or disclosed within or outside the Postal Service, except for Postal Service operations and law enforcement purposes as specified in Title 39 of the *Code of Federal Regulations* (CFR) 233.3 and chapter 2 of the *Administrative Support Manual.*

2-3 Federal Laws

2-3.1 Postal Reorganization Act

The Postal Service is restricted from sharing customer or mailing information by the Postal Reorganization Act, Title 39 of the United States Code (U.S.C.). Under 39 U.S.C. 412, the Postal Service cannot make available to the public, by any means or for any purpose, any mailing or other list of names or addresses (past or present) of customers or other persons, unless specifically permitted by statute.

2-3.2 Privacy Act

The Privacy Act provides privacy protections for personal information maintained by agencies.

A summary of the Privacy Act follows.

a. *General.* The Privacy Act of 1974, 5 U.S.C. 552a, applies to federal agencies, including the Postal Service. The Act provides privacy protections for personal information that agencies maintain in a

"system of records." A system of records is a file, database, or program from which personal information is retrieved by name or other identifier. A full description of Privacy Act protections and Postal Service systems of records is contained in the Appendix. Postal Service regulations regarding the Privacy Act are located in 39 CFR 266 and 268. Procedures relating to the Privacy Act are described in chapter 3.

b. *Requirements.* When an agency maintains a system of records, it must publish a notice that describes the system in the *Federal Register.* The notice must document how the agency manages personal information within the system. This includes how information is collected, used, disclosed, stored, and discarded. It also includes how individuals can exercise their rights to obtain access to and amend information relating to themselves contained in the system. The Privacy Act further requires that the Postal Service provide an appropriate privacy notice to individuals when they are asked to provide information about themselves.

c. *Penalties.* The Privacy Act provides criminal penalties, in the form of fines of up to $5,000, for any officer or employee who:

(1) Willfully maintains a system of records that contains information about an individual without giving appropriate notice in the *Federal Register;* or

(2) Knowing that disclosure is prohibited, willfully discloses information about an individual in any manner to any person or agency not entitled to receive it.

The Privacy Act also provides criminal penalties, in the form of fines of up to $5,000, for any person who knowingly and willfully requests or obtains under false pretenses any record about another individual.

2-3.3 Freedom of Information Act

The FOIA, 5 U.S.C. 552, provides the public with a right of access to records (hard copy and electronic), that are maintained by federal agencies, including the Postal Service. The FOIA contains exemptions that authorize the withholding of certain information. Postal Service regulations implementing the FOIA are located in 39 CFR 265. Postal Service procedures governing the disclosure of information under FOIA are described in chapter 4.

2-3.4 E-Government Act of 2002

The E-Government Act of 2002, 44 U.S.C. Chapter 36, is intended to protect privacy in the provision of electronic government services and applies when agencies collect personal information in new or modified information technology systems. The Postal Service has adopted policies to comply voluntarily with the Act's privacy provisions. This includes requirements to conduct privacy impact assessments, to post privacy policies on Web sites used by the public, and to translate privacy policies into a standardized machine-readable format.

2-3.5 Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLB), Title V, 15 U.S.C. 6801–6827, governs the treatment of personal information when certain financial services are provided in the private sector. The GLB requires that customers be given notice about data practices and choices as to whether data can be shared with unaffiliated parties. Examples of financial services include banking activities or functions; wire or monetary transfers; printing, selling, or cashing checks; or providing credit services. Financial services do not include accepting payment by check or credit card issued by another entity. The Postal Service has adopted policies to comply voluntarily with GLB for its products and services that would be considered financial services if offered by a private sector company.

2-3.6 Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501–6505, is intended to protect children's privacy on the Internet. COPPA applies to operators of commercial Web sites who direct the Web site to, or knowingly collect information from, children under the age of 13. COPPA requires such operators to provide notice of data practices and to obtain parental consent before collecting children's personal information, unless certain exceptions apply. The Postal Service has adopted policies to comply voluntarily with COPPA in its Web site operations.

2-4 Federal Agency Guidelines

The Federal Trade Commission (FTC) and the Office of Management and Budget (OMB) have issued guidelines related to privacy and data management practices for the private sector and federal agencies, respectively. The Postal Service has adopted policies and practices based on these guidelines.

2-4.1 Federal Trade Commission Privacy Principles

The FTC has established fair information principles that it recommends the private sector provide to customers. The principles are notice, choice, access, security, and redress. Notice provides customers with information about the organization's data management practices before personal information is collected from them. Choice is about obtaining the customer's consent before using the information for a purpose other than the purpose for which it was collected (i.e., secondary uses). Secondary uses include other internal uses, such as to cross- or up-sell different products, or to share the information with third parties. Access provides customers a way to access and amend information the organization maintains about them. Security involves measures to protect against loss and the unauthorized access or disclosure of information. Redress provides a means by which customer questions and complaints can be received and processed.

2-4.2 Office of Management and Budget Privacy Guidelines

Since the Privacy Act was passed in 1974, the OMB has developed numerous guidelines about protecting the privacy of personal information collected by government agencies. The guidelines are outlined in the following publications:

- Implementing the Privacy Provisions of the E-Government Act of 2002 (9/2003)
- Guidance on Inter-Agency Sharing of Personal Data — Protecting Personal Privacy (12/2000).
- Privacy Policies and Data Collection on Federal Web Sites (6/2000).
- Guidance and Model Language for Federal Web Site Privacy Policies (6/1999).
- Privacy and Personal Information in Federal Records (1/1999).
- Privacy Act Implementation, Guidelines and Responsibilities (7/1975).

OMB emphasizes the Privacy Act and its role in new technologies. OMB gives particular attention to certain technologies on agency Web sites, including Web analysis tools such as cookies, and requires notice and agency head approval for their use.

2-5 Postal Service Policies

2-5.1 Customer Privacy Policy

The Postal Service customer privacy policy provides privacy protections for all of its customers, appropriately tailored for each customer segment (consumers and businesses). The policy applies to customer information collected via all channels, including hard copy forms, call centers, e-mail, and *usps.com*. The policy also includes specific notice and limitations regarding Web analysis tools used on *usps.com*. A full statement of the customer privacy policy is available via a link on *usps.com*, in the footer on each page, or by contacting the CPO at the address in section 1-4.2.4. The Postal Service has also published Privacy Act systems of records for customer information it collects and maintains. These systems of records are contained in the Appendix. Procedures relating to privacy are described in chapter 3.

2-5.2 Marketing E-mail Policy

The Postal Service uses e-mail to communicate with current and potential customers. The Postal Service marketing e-mail policy applies when the Postal Service or one of its suppliers sends an e-mail message to a customer or prospective customer marketing a product that is different from a product the customer may already receive from the Postal Service. Procedures relating to the policy are available in MI AS-350-2004-4, *Marketing E-mail.*

2-5.3 Supplier Policy

Suppliers and business partners must adhere to the Postal Service privacy policies if they have access to customer, employee, or other individuals' information; help to build or operate a Postal Service Web site; or conduct a marketing e-mail campaign. The contracts and agreements, whether or not covered by Postal Service purchasing regulations, must include an appropriate privacy clause(s). Reference purchasing regulations at 39 CFR Section 601. To reference purchasing guidelines and privacy protection clause 1-1 go to *http://about.usps.com/manuals/pm/welcome.htm.*

2-5.4 Monitoring of Postal Service Equipment

The Postal Service reserves the right to access and monitor computer use and information contained in or passing through its information resources, including the contents of all messages sent over its electronic messaging systems. The Corporate Information Security Office and the Privacy Office have established policies and procedures to conduct monitoring, which are contained in MI AS-870-2007-7, *Electronic Messaging.*

This page intentionally left blank

3 Protecting Individual Privacy

3-1 Overview

3-1.1 General Policy

In its normal course of operation, the Postal Service collects, maintains, and uses information that relates to, or could be used to identify, individuals ("personal information"). Both federal law and postal policies regulate how this information is collected and maintained. The Privacy Act of 1974 establishes principles, standards, and safeguards for the collection, maintenance, and dissemination of personal information by federal executive agencies and the Postal Service. Additionally, the Postal Service has promulgated a series of programs, processes, and policies that protect the privacy of individuals, including customers and employees.

3-1.2 Scope

This chapter applies to all personal information maintained by the Postal Service, its agents, and its contractors or suppliers.

3-1.3 Implementation

The Privacy and Records Management Office, in partnership with Information Security, participates in the Business Impact Assessment (BIA) and the Cloud Computing Impact Assessment (CCIA) processes. The BIA is an internal evaluation that predicts the consequences of disruption of a business function. Within this process, the sensitivity, criticality, privacy compliance, information security needs, and information retention requirements of a new or existing information resource are determined. The BIA is the first phase of the Information Security Assurance (ISA) process, which protects information contained in the resource through its lifecycle.

The CCIA is an internal evaluation that addresses the sensitivity, criticality, privacy compliance, information security needs, and information retention requirements of new or existing technology solutions that use cloud computing. The BIA and CCIA ensure privacy compliance and also document the sensitivity of the system, which contributes to establishing a security plan. The executive sponsor of the system is responsible for completing and adhering to the BIA or CCIA. Completed BIAs and CCIAs must be submitted to, and approved by, the Chief Privacy and Records Management Officer, the business owner, and the manager of the Corporate Information Security Office.

3-2 Maintaining a System of Records

3-2.1 Policy

In general, when the Postal Service maintains, collects, uses, or disseminates information on individuals ("personal information"), such information must be covered by a "System of Records." The term System of Records (SOR) is a formal legal concept grounded in the Privacy Act that is distinct from a similar term used in the field of data management. The Postal Service must advise the public about each SOR it has established by publishing a notice in the *Federal Register*. The Postal Service also publishes descriptions of its SORs in the Appendix to this handbook. Personal information can only be used by the Postal Service (or its agents or suppliers acting on behalf of the Postal Service) for the purposes that are listed in the SOR.

The Postal Service has published several SORs that are organized based on the subject matter of the personal information the organization is maintaining (e.g., personnel records, customer change-of-address records). Each SOR contains the following information:

- Categories of Records in the System (what types of personal information the Postal Service is collecting);
- Categories of Individuals Covered by the System (the types of individuals whose information is covered by the system);
- Record Source Categories (the persons or entities from whom the Postal Service is collecting the personal information);
- Purposes (the reasons or purpose(s) the Postal Service is collecting the personal information, including how the information will be used);
- Routine Use (a concise statement that identifies the persons to whom the Postal Service may disclose the information and for what reasons — each SOR has several routine uses);
- Authority for Maintenance of the System (the federal laws or executive orders that allow the Postal Service to collect and use the information);
- System Location (the locations or facilities where the information is maintained);
- Retention and Disposal (a general description of the policies for retaining and disposing of records covered by the system, which must be consistent with the associated records control schedules); and
- Storage, Retrievability, and Safeguards (the policies regarding the protection, retrieval, and disposal of the information).

Most, but not all, Postal Service records that contain personal information must be "covered" by an SOR, regardless of whether the information is in hard copy or electronic format. Additionally, a single SOR can encompass multiple, separate groupings or collections of records. If you are unsure whether the records you maintain are covered by an SOR, reference the Appendix or the associated records control schedule. Records control schedules can be found in ERIMS (*https://erims.usps.gov/erims/erims*). The

Privacy and Records Management Office can assist you in determining which, if any, SOR applies or whether a new SOR should be created or an existing SOR modified.

3-2.2 Establishing, Changing, or Deleting an SOR

The Privacy and Records Management Office manages the process for creating, amending, or deleting an authorized SOR. The need for the establishment, change, or deletion of an SOR can be identified during the BIA or CCIA process (see 3-1.3). However, these changes can be made at any time to respond to organizational needs. Contact the Privacy and Records Management Office for assistance under the following circumstances:

a. You are considering collecting and maintaining (e.g., using, processing, disclosing) information about customers, employees, or other individuals in a manner that is not currently described in an existing SOR as documented in the relevant records control schedule for your database, file, or other information system.

b. You are making any of the following changes to your program or initiative that requires corresponding amendments to the relevant SOR:

   (1) Changing the types of individuals or the scope of the population on whom the records are maintained.

   (2) Expanding or reducing the types of information maintained (i.e., the data elements).

   (3) Amending, adding to, or deleting a purpose for which information is collected and maintained.

   (4) Changing the manner in which the records are stored or retrieved to change the nature or scope of these records (e.g., change from a manual to an automated system).

   (5) Changing or adding a “routine use” (authorized disclosures from the system).

   (6) Changing the name or location of a system owner.

   (7) Changing the retention period.

c. You are currently collecting and maintaining information on individuals but the collection and maintenance is not clearly described by an existing SOR as documented in the relevant records control schedule and BIA.

3-2.3 Timeframe for Changes to SORs

Changes to an SOR can involve a lengthy administrative process, which includes internal clearance by the Chief Privacy and Records Management Officer, each “system owner” (typically a Vice President), and any other relevant internal stakeholder, and, in some cases, Government Relations. Advance notice of the changes may then need to be provided to our Congressional oversight committees and the Office of Management and Budget before being published in the *Federal Register*. Additionally, certain SOR changes require that the Postal Service give the public 30 days to submit comments on the proposal before the changes can be implemented.

As a result, the process for establishing or amending an SOR can take anywhere from 2 to 6 months to implement. Contact the Privacy and Records Management Office as early as possible to ensure that your project or initiative is not unnecessarily delayed in order to meet regulatory requirements.

3-3 Collecting Personal Information

3-3.1 Collection by the Postal Service

The Postal Service may only collect personal information that is relevant or necessary to carry out a purpose authorized by federal statute or by executive order as documented in the relevant SOR. To the greatest extent practical, the Postal Service must collect personal information directly from the individual.

The Postal Service cannot discriminate against any individual who fails to provide personal information unless such information is required for a service, product, or program in which the individual has requested or wishes to participate. Finally, the Postal Service may not require an individual to provide his or her Social Security number or deny a right, privilege, or benefit because of an individual's refusal to furnish the number, unless it must be provided pursuant to federal law. Before collecting Social Security numbers from individuals, consult with the Privacy and Records Management Office.

3-3.2 Collection by Contractors

Contractors (including suppliers) working under a Postal Service contract may also, in the course of performing the contract, collect and maintain personal information. To the extent that a contractor is collecting information on behalf of the Postal Service, or to fulfill a Postal Service function or duty, the privacy requirements that apply to the Postal Service also apply to the contractor unless otherwise agreed to in writing. Refer to 3-6.1 for these requirements.

3-3.3 Prohibition on Collecting Information Related to Exercise of First Amendment Rights

The Privacy Act broadly prohibits the Postal Service from collecting or maintaining records describing or relating to how an individual exercises his or her rights under the First Amendment of the U.S. Constitution. Prohibited records include, among other things, those that describe a person's political, ideological, or religious affiliations and associations. There is an exception to this rule if the Postal Service is expressly authorized by statute to maintain such records, if the individual has expressly authorized the Postal Service to maintain the information, or maintaining the records is pertinent to and within the scope of an authorized law enforcement activity. If you are concerned or suspect that you are collecting information that relates to an individual's exercise of his or her First Amendment rights, contact the Privacy and Records Management Office as soon as possible.

3-4 Providing a Privacy Notice to Individuals

3-4.1 Purpose of Providing Notice

Whenever the Postal Service asks a customer, employee, or other individual to submit personal information to the Postal Service, the Postal Service must provide the individual with a privacy notice. A privacy notice is a clear and concise statement that explains, among other things, how the Postal Service intends to use the information that the individual is providing and to whom such information may be disclosed. Providing a privacy notice helps to ensure that the individual can make an informed decision regarding whether to provide personal information to the Postal Service. Privacy notices are essential for ensuring that the Postal Service is transparent to the individual with regard to its use of personal information and for maintaining compliance with federal laws. Such notices must be provided any time the Postal Service is collecting information from individuals, even if the information will not be maintained in connection with the individual's name or personal identifier (i.e., anonymous information).

3-4.2 Content of the Privacy Notice

Each privacy notice must contain the following information:

- The purpose or reason that the Postal Service is collecting the personal information (for example, "to provide a service to the customer" or "to fulfill an employee's request").
- Whether providing the information is mandatory or voluntary. Unless there is a specific law that requires that an individual submit his or her personal information, the submission must be considered "voluntary."
- A statement describing what will or may happen if a person decides not to submit his or her personal information. For example, if a customer does not provide the requested information, the Postal Service may be unable to provide service to the customer.
- A brief description of the persons or entities outside the Postal Service to whom the personal information may be disclosed. Typically, these persons and organizations are listed in the System of Records that has been designated for the collection or maintenance of the personal information.
- A citation to each relevant law, statute, or executive order that authorizes the Postal Service to collect the personal information.
- A link to the USPS Privacy Policy available on *usps.com*.

Because in most cases the personal information must be covered by an SOR, the content of the privacy notice must closely align with the corresponding SOR. In all cases, the Privacy and Records Management Office can assist you in drafting the notice for your program, application, or initiative.

3-4.3 Method of Providing Notice

The privacy notice must be provided to the individual in a manner that is appropriate given the context of the interaction. Below are some common locations in which individuals may be asked to submit personal information and corresponding guidelines on how the privacy notice must be provided in those situations.

Contact Point	Procedures for Providing a Privacy Notice to Individuals
In Person (e.g., retail, interviews)	■ A privacy notice document may be provided to the customer or the notice can be read aloud. ■ If the notice is read aloud to the individual, make a note that the notice was provided orally and save that note with the customer's personal information as proof that the notice was provided. ■ If the privacy notice is provided orally, the individual must be provided with an opportunity to receive a hard copy of the USPS Privacy Policy either at the contact point or through the mail.
Hard Copy Forms	■ A written privacy notice must appear on or adjacent to the form close to where personal information will be entered by the individual. ■ Alternatively, a separate written notice can be provided before the individual is asked to submit his or her personal information.
Telephone	■ Provide callers with a privacy notice using an automated system or by providing the notice orally. If an automated system is used, the system must deliver the notice when the caller is transferred to an option where personal information may be collected. ■ If a caller requests additional information, the agent must mail or email the caller a copy of the privacy notice. ■ Alternatively, postal personnel responding to a call may provide the notice orally. ■ If the privacy notice is provided orally, the individual must be provided with an opportunity to receive a hard copy of the USPS Privacy Policy either at the contact point or through the mail.
Online/Website	■ Provide a privacy notice on a portion of the page that is close to the location where the personal information is being collected. If such placement is not feasible or desirable, a pop-up box may be used that contains the text of the notice.

Contact Point	Procedures for Providing a Privacy Notice to Individuals
Email	■ If personal information may be collected as a result of an email interaction, provide a privacy notice in the same email that solicits the personal information or in a communication that precedes the collection of the information.

3-5 Respecting Communication Preferences

3-5.1 Policy

The Postal Service voluntarily follows the guidelines set forth by the Federal Trade Commission (FTC) when the Postal Service wants to contact individual customers in order to provide them with information for reasons that differ from the original reason that the customer provided his or her personal information. For example, these guidelines apply when the Postal Service wants to send the customer marketing or advertising communications that relate to a different product or service than the customer has previously selected. Additionally, these guidelines apply when the Postal Service wants to share personal information externally with third parties other than Postal Service contractors and service providers. Refer to 3-9 for policies related to collecting contact information from businesses.

3-5.2 Providing Choice to Individual Consumers

The Postal Service uses an “opt in” standard for individual customers, which means that customers must affirmatively authorize the Postal Service to use or share personal information for these “secondary” purposes. Additionally, the Postal Service must provide individual customers with the ability to select or change their preferences in a consumer-friendly manner. Preferences can be documented through a checkbox on a hard copy form or webpage, or through another means that is convenient to the customer. The Postal Service must give customers the ability to modify their previous decisions so that their current choices and preferences are respected.

3-5.3 Sending Marketing Email

The Postal Service’s marketing email policy applies when the Postal Service, or one of its suppliers, sends an email message to a customer or prospective customer that markets a different product or service than the consumer or business customer may already receive from the Postal Service. Managers or employees intending to send a marketing email must submit the email through the Law Department Ad Review process and follow the procedures for notice and choice provided in the CAN-SPAM Act. Complete procedures are available in Management Instruction (MI) AS-350-2004-4, *Marketing E-mail*.

3-6 Requests for Amendment

3-6.1 Policy

Customers, employees, or other individuals may request an amendment of information about themselves that is maintained by the Postal Service. A customer who is a registered user on *usps.com* may amend his or her personal profile through his or her customer account.

3-6.2 Minor v. Significant Amendments

Individuals may submit a verbal request to the records custodian if the requested change concerns a minor error or correction. A minor amendment includes correcting a misspelling, misprint, or mistake in computation. All other types of changes are considered to be significant amendments. Individuals must submit a written request to the records custodian for a significant amendment to his or her record.

3-6.3 Requirements for the Requester

Written requests must include a certification of identity (see 4-3.2.5) and be submitted in accordance with the procedures described in the applicable system of records in the Appendix. Requesters must state the reason or reasons for requesting the change. Possible reasons may include, but are not limited to:

- Maintaining the relevance of the record;
- Ensuring the accuracy of the record;
- Ensuring that the record is current and timely; and
- Ensuring the completeness of the record.

3-6.4 Requirements for the Responder

The person tasked with responding to the request must follow these procedures:

1. Acknowledge the request. Within 10 days (excluding weekends and federal holidays) of receipt of any written request to amend a record, acknowledge the request in writing.
2. Act on the request. Within 30 days (excluding weekends and federal holidays) of receipt of any written request to amend a record, verify the identity of the requester in accordance with the notification procedures described in the applicable systems of records.
3. Obtain information. Ask the requester for any additional information necessary for action on the request. Also, if needed, ask postal personnel for additional information to determine whether amendment is appropriate.
4. Amend the information as necessary. Correct or eliminate any information found incomplete, inaccurate, untimely, or irrelevant.
5. Respond to the request. For requests submitted in writing, advise the requester in writing of any change that was made to the record and,

where practical, supply a courtesy copy of the revised record. Send a revised record to any person or agency to whom a disclosure has been made under 4-3.3.3(b.) through (e.), as listed in the accounting of disclosures made for that record (see 4-3.5).

3-6.5 Denials and Appeals

Notify the requester in writing if any requested changes are denied in whole or in part, including the reasons for the denial. The denial must include notification that the requester may submit a statement of disagreement to be appended to the disputed record or that he or she may appeal the decision. Appeal procedures are the same as those for notification and access requests (see 4-3.4; see 4-3.2.12(e.)((4)) for appeal language).

3-7 Legal Agreements Involving Personal Information

The Postal Service routinely enters into agreements with businesses, agencies, or other organizations that involve the collection, maintenance, transfer, or exchange of personal information. These include contracts maintained by Supply Management, data sharing agreements such as Interagency Agreements (IAAs) or Memoranda of Understanding (MOUs), and certain programs that involve the automated comparison of personal data internally or between the USPS and another organization ("computer matching programs"). These three circumstances are described in the following sections.

3-7.1 Collection by Contractors or Suppliers

If a contractor operates a system of records on behalf of the Postal Service, the privacy regulations as described in this chapter are applicable unless otherwise agreed to in writing by the parties. If the contractor has access to personal information, such information may only be used for the purposes of the contract and the contractor must restrict access to the information to only its employees who need the information in order to perform work under the contract, and those employees must sign a nondisclosure agreement. The contractor must also develop a security plan to protect personal information and the contractor must notify the Postal Service if there is an actual or suspected breach of personal information. Complete requirements are set forth in Clause 1-1 of the *Supplying Principals and Practices*. Also see the purchasing regulations in 39 CFR Part 601.

3-7.2 Data Sharing Agreements

In order to accomplish certain business, regulatory, investigatory, and other objectives, the Postal Service enters into legal agreements that involve the transfer or exchange of data between the Postal Service and third-parties such as federal agencies, corporations, or other organizations. This includes, among other things, statistical matching, comparison of aggregate data, law enforcement investigative matches, tax administration matches, and security clearance background checks. To ensure the privacy and security of

personal information transferred or exchanged pursuant to these agreements, these agreements generally incorporate Postal Service policies pertaining to privacy, security, and confidentiality of data. The Privacy and Records Management Office reviews and advises on the privacy, disclosure, and records management provisions of data transfer agreements.

3-7.3 Computer Matching Programs

A computer matching program is one that involves a computerized comparison of two sets of personal data, including two systems internal to the Postal Service or a comparison between the Postal Service's data and data from another entity. If a data-sharing agreement requires the Postal Service or the partner organization to conduct a computer match of personal data, the parties must enter into a Computer Matching Agreement that meets special requirements in the Privacy Act. The Postal Service Data Integrity Board is responsible for the review and approval of all Postal Service computer matching activities. The Privacy and Records Management Office manages the approval process for Computer Matching Agreements and is available to opine on whether a program or initiative that involves the transfer or exchange and use of personal information triggers the requirements of the Privacy Act. Submit any proposals that involve the computer matching of personal data at least 6 months in advance of the anticipated starting date to allow time for review and publication requirements. See MI AS 350-2007-1, *Computer Matching Programs,* and 39 CFR 266.9 for more information.

3-8 Special Privacy Requirements

There are some specific circumstances in which additional privacy requirements are applicable, including when the Postal Service maintains the names and addresses of individuals or when the Postal Service maintains a customer website. These situations not only implicate specific privacy requirements, but also trigger additional procedures that protect customers and their information.

3-8.1 Specific Prohibitions Regarding Names and Addresses

The Privacy Act prohibits the Postal Service from selling or renting any individual's name or address to anyone for any reason, including to other people, agencies, or businesses. Additionally, the Postal Reorganization Act (PRA) prohibits the Postal Service from publicly disclosing lists of customer names and lists of customer addresses for any reason. The only exception to these rules is if there is a law that specifically authorizes the Postal Service to sell, rent, or disclose such information. For example, if the information is required to be disclosed under the Freedom of Information Act (FOIA), the disclosure of such information is authorized. Contact the Privacy and Records Management Office if questions arise.

3-8.2 Operating a Customer Website

Websites used by customers, regardless of whether they collect customer information, must comply with the customer privacy policy on *usps.com*, including with regard to use of Web analysis tools such as cookies or Web beacons. If the website provides links to external websites, follow the procedures in MI AS-610-2012-3, *Web Site Affiliation Program.*

3-9 Business Information

3-9.1 Scope

This section explains what type of privacy notice must be provided when the Postal Service collects information from corporations, organizations, and other entities that are not individuals. The term "business customer" will be used to refer to these entities. Although, there are fewer privacy obligations with regard to providing notice to business customers, the Postal Service follows the guidelines below as best practices.

3-9.2 Content of Notice

The notice provided to business customers is a brief, concise statement that directs the submitter to the official USPS Privacy Policy.

Example: For more information regarding our privacy policies, visit *www.usps.com/privacypolicy*.

3-9.3 Method of Providing Notice

The privacy notice for business customers must be provided in a manner appropriate to the context of the information being collected. Here are some common examples:

Contact Point	Procedures for Providing a Privacy Notice
In Person (e.g., retail, interviews)	The notice may be printed on a sheet and handed to the customer's representative or the notice can be read aloud to the representative.
Hard Copy Forms	The written notice must appear on or adjacent to the form close to where the information is collected. Alternatively, a separate written notice can be provided.
Telephone	Provide callers with a notice using an automation system or by providing the notice orally.
Online/Social Media	Provide notice on a portion of the page that is close to the area where the information is being collected. If such placement is not feasible or desirable, a pop-up box may be used that contains the text of the notice.
Email	Provide notice in the same email that solicits the information or other communication that precedes the collection of the information.

3-9.4 Policy on Communicating with Business Customers

The Postal Service voluntarily follows the guidelines set forth by the Federal Trade Commission (FTC) for contacting business customers to communicate with them or send them information for reasons that differ from the original reason that the business provided its contact information to the Postal Service. For example, these guidelines apply when the Postal Service wants to send the business customer marketing or advertising communications that relate to a different product or service than the customer has previously selected. These guidelines also apply when the Postal Service wants to share the business's information externally with third parties other than Postal Service contractors and service providers. The Postal Service may use an "opt out" standard for business customers, which means that business customers must affirmatively decline to allow the Postal Service to use its information for these "secondary" purposes.

3-9.5 Providing Choice to Business Customers

The Postal Service must provide business customers with the ability to state their preferences in a consumer-friendly manner. Preferences can be documented through a checkbox on a hard copy form or on a web page, or through another means that is convenient to the customer. The Postal Service must give customers the ability to modify their previous decisions so that their current choices and preferences are respected. Accordingly, direct customers to register with *usps.com* and create a profile that will allow them to select and amend their choices.

4 Records Notification, Access, and Disclosure Procedures Under the Privacy Act and Freedom of Information Act

4-1 General

4-1.1 Privacy Act of 1974

The Privacy Act of 1974 (Privacy Act) (5 U.S.C. 552a):

a. Requires the Postal Service to notify an individual, upon request, whether records about the individual exist in a Postal Service system of records, unless protected from such notification by law.

b. Requires the Postal Service to provide an individual, upon request, access to records about the individual in a Postal Service system of records, unless otherwise protected from such access by law.

c. Only permits or requires the Postal Service under limited circumstances to disclose to a third party, upon request, records about an individual in a Postal Service system of records.

The procedures for an individual to request notification of or access to records about the individual in a Postal Service system of records under the Privacy Act and Postal Service policy are available at *https://about.usps.com/who-we-are/foia/welcome.htm*.

This chapter provides the procedures for a records custodian or other Postal Service employee to follow when responding to a notification, access, or disclosure request under the Privacy Act.

4-1.2 Freedom of Information Act

The Freedom of Information Act (FOIA) (5 U.S.C. 552) requires the Postal Service to disclose its records to the general public, upon request, unless protected from such disclosure by law.

The procedures for the general public to submit a request for disclosure of records under the FOIA and Postal Service policy are available at *https://about.usps.com/who-we-are/foia/welcome.htm.*

This chapter provides the procedures for a records custodian or other Postal Service employee to follow when responding to a request under the FOIA.

4-1.3 Additional Guidance for Responding to Requests Under the Privacy Act and FOIA

4-1.3.1 Additional Postal Service Resources

a. Records custodians and other Postal Service employees should seek guidance as necessary from, as appropriate, their FOIA coordinator, their FOIA requester service center, the Privacy and Records Management Office, or their legal office when responding to notification or access requests under the Privacy Act or disclosure requests under the FOIA.

b. Postal Service's regulations implementing the Privacy Act at 39 CFR Part 266.

c. Postal Service's regulations implementing the FOIA at 39 CFR Part 265.

4-1.3.2 Department of Justice Guidance

a. *Overview of the Privacy Act of 1974* available at *https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition*.

b. *Guide to the Freedom of Information Act* available at *https://www.justice.gov/oip/doj-guide-freedom-information-act-0*.

4-1.3.3 Office of Management and Budget Guidance

a. Privacy Act Guidelines, 40 *Federal Register* 28949 (July 1, 1975).

b. FOIA Uniform Fee Schedule and Guidelines, 52 *Federal Register* 10012 (March 27, 1987).

4-2 Public Records and Information Under FOIA

4-2.1 Records Available in Reading Rooms

4-2.1.1 Responsibilities of Records Custodians

Each records custodian is responsible for:

a. Identifying which of its records are required under the FOIA to be made available to the general public in the Postal Service's electronic reading room, including, but not limited to records that have previously been disclosed under the FOIA and meet one of the following conditions:

(1) Because of the nature of their subject matter have or are likely to become the subject of subsequent requests for substantially the same records.

(2) Have been requested three or more times under the FOIA.

b. Identifying additional records of interest to the general public that are appropriate for disclosure to the general public.

c. Ensuring the records identified in paragraphs a. and b. are made available in the Postal Service's electronic reading room.

4-2.1.2 Reading Rooms

The records available to the general public in the Postal Service's public and electronic reading rooms in compliance with the FOIA or within the discretion of the Postal Service include, but are not limited to, the following:

a. *Public Reading Room.* The following records are available for inspection and copying by the general public in the public reading room in the Postal Service Headquarters library:

(1) All final opinions and orders made in the adjudication of cases by the judicial officer and administrative law judges.

(2) All final determinations pursuant to 39 U.S.C. 404(b) to close or consolidate a Post Office or to disapprove a proposed closing or consolidation.

(3) All advisory opinions about the private express statutes issued under 39 CFR 310.6.

(4) All supplier disagreement decisions.

(5) Postal Service manuals, instructions, and other publications that affect the general public that are not listed for sale to the general public.

(6) Records that were or were likely to be routinely processed and disclosed under the FOIA after March 31, 1997.

b. *Electronic Reading Room. R*ecords available in the public reading room described in paragraph a. that were created on or after November 1, 1996, are also maintained in the electronic reading room.

In addition, indexes of certain records are maintained in the public and electronic reading rooms, and otherwise made available to the general public to the extent required by the FOIA or within the discretion of the Postal Service.

The Postal Service's electronic reading room may be accessed at *http://about.usps.com/who-we-are/foia/readroom/welcome.htm*.

Postal Service manuals, instructions, and other publications that affect the general public that are available to the general public in the public and/or electronic reading rooms are also available for inspection by the general public in many Post Offices and other Postal Service facilities. Postal Service publications that are not available to the general public in the public and/or electronic reading rooms or Postal Service facilities or listed for sale to the general public may be requested by the general public pursuant to the FOIA disclosure provisions (see 4-4).

Note: Records available to the general public may contain redactions to the extent permitted by the FOIA.

4-2.2 Other Information Available to the Public

4-2.2.1 Public Information About Postal Service Customers

The name or address of a specifically identified Postal Service customer is disclosed to the general public upon request as follows:

a. *Business or Organization Change of Address.* Requests for the new address of a specific business or organization must be submitted to the Postmaster serving the last known address. There is no fee for providing this information.

b. *Name and Address of Permit Holder/Name of Person Applying for Permit on Holder's Behalf.* The name and address of the holder of a particular bulk mail permit, permit imprint, or similar permit (but not including postage meter licenses) or name of a person applying for a permit on behalf of a holder is disclosed to the general public under the conditions specified in 39 CFR 265.14(d)(2). Requests must be submitted to the Postmaster of the location noted on the permit imprint. There is no fee for providing this information.

c. *Name and Address of Postage Evidencing System User.* The name and address of an authorized user of a postage meter or PC Postage product (postage evidencing systems) printing a specified indicium is disclosed to the general public under the conditions specified in 39 CFR 265.14(d)(3) and Appendix, section E, USPS 870.200, Routine Uses of Records in the System. Such requests must include the original copy of the envelope or wrapper on which the indicium is printed and a copy or description of the contents. There is a fee for this service. Lists of users of postage evidencing systems may not be disclosed. All requests must be sent to:

POSTAGE TECHNOLOGY MANAGEMENT
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW RM 3660
WASHINGTON, DC 20260

d. *Commercial Mail Receiving Agency Address.* The address of a commercial mail receiving agency is disclosed to the general public to the extent provided in 39 CFR 265.14(d)(9)(ii), 5-2.d(3)(a), and Exhibit 5-2a, *Address Disclosure Chart*.

e. *Business/Residence Location.* If the location of a residence or business is known to a Postal Service employee, the employee may disclose it or give direction to it to the general public under the conditions specified in 39 CFR 265.14(d)(8) and 5-2.d(2).

4-2.2.2 Public Information About Postal Service Employees

The following information about Postal Service employees is disclosed to the general public upon request to the extent provided in 39 CFR 265.14(e), 5-2.b(1), and 5-2.b(3):

a. The name, job title, grade, salary, duty station, and dates of employment of a current or former employee.

b. A listing of employees working at a particular Postal Service facility.

4-3 Responding to Notification, Access, and Disclosure Requests Under the Privacy Act

4-3.1 Responsibility for Responding to Notification, Access, or Disclosure Requests Under the Privacy Act

Ordinarily, it is the responsibility of the relevant records custodian (or designee) to respond to an initial notification, access, or disclosure request under the Privacy Act in accordance with the procedures in 4-3. For the purpose of 4-3, "records custodian" means any Postal Service employee who responds to a notification, access, or disclosure request under the Privacy Act. Any misdirected notification, access, or disclosure request must be promptly forwarded to the appropriate records custodian identified in the system of records for response, and notification of the referral provided to the requester.

4-3.2 Responding to Requester's Request for Notification of or Access to Records About Himself or Herself Under the Privacy Act

4-3.2.1 Evaluating Under the FOIA a Request for Access by Requester to His or Her Records

As provided in 4-3.2.2.b and 4-3.2.9.b, the records custodian must, in some scenarios, evaluate a request for access to records about the requester under the FOIA's disclosure provisions (see 4-4), as well as under the Privacy Act's access provisions. This is the case even if the request does not cite the FOIA. This procedure provides the requester with the greatest access to records pertaining to the requester.

Note: A requester's access to records about himself or herself under the FOIA is different than under the Privacy Act. A requester may qualify as a *person* under the FOIA (broader definition) (see 4-4.5.c) but not as an *individual* under the Privacy Act (narrower definition) (see 4-3.2.2.c). In addition, the requested records may qualify as *records* under the FOIA (broader definition) (see 4-4.5.d) but not qualify as *records* about the requester in a Postal Service *system of records* under the Privacy Act (narrower definition) (see 4-3.2.2). Further, the FOIA exclusions/exemptions (see 4-4.22 and 4-4.24) are different than the Privacy Act exemptions (see 4-3.2.9); although, in some cases, the exemptions are similar but not identical.

	Freedom of Information Act	**Privacy Act of 1974**
Citation for laws	Title 5 U.S.C. 552	Title 5 U.S.C. 552a
Citations for Postal Service regulations	■ Title 39 CFR 265 ■ Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management* (Chapters 4 and 5).	■ Title 39 CFR 266 ■ Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management* (Chapter 3 and Appendix).
Nature and purpose of the statute	■ The FOIA requires the Postal Service to disclose upon written request any record that is not covered by a FOIA exemption. The FOIA keeps the public informed about what our government is doing.	■ The Privacy Act (PA) grants individuals a right of access to their own records and imposes fair record-keeping requirements on the Postal Service. The PA balances the government's need to know and the individual's right to privacy.
Coverage	■ All agency records.	■ All agency records covered by a Privacy Act system of records (SOR) (a group of records kept about individuals and retrieved by a personal identifier). See the Appendix in Handbook AS-353.
Access provisions	■ Any person can gain access to non-exempt records.	■ Only to the subject of the record or appropriate designee. ■ Applies only to U.S. citizens and aliens lawfully admitted for permanent residence. ■ Access may be granted to third parties through "exceptions" (e.g., routine uses, authorized disclosures).
Fees	■ Search, review, and duplication fees based on identity of the requester.	■ Fees limited to duplication costs.
Records searches	■ Reasonable search of all records created or maintained by the USPS, including those in any Privacy Act system of records (SOR).	■ Search is limited to records contained in a USPS SOR (unless there is reason to believe that records exist in non-Privacy Act files).
Time limits	■ The FOIA states that agencies must respond within 20 working days; 10 additional working days granted in unusual or exceptional circumstances.	■ Acknowledge request within 10 working days of the request, provide records as soon as practical, and give the requester a date of availability if records are not immediately available.
Reasons to appeal Agency's initial response	■ Adequacy of search; ■ Failure to comply with time limits; ■ Denial of information in full or in part; and ■ Denial of fee waiver or expedited processing request.	■ Denial of access; and ■ Denial of amendment request.

4-3.2.2 Determining Qualification as a Covered Individual, Record, and System of Records

a. *General.* In order for a notification or access request to be further considered under the Privacy Act, the requester must qualify as an *individual*, and the records inquired about or requested must qualify as *record*s about the requester in a Postal Service *system of records*.

b. *Evaluating Under the FOIA Requester's Access Request for His or Her Records.* If the requirements in paragraph a. are not met for an access request (e.g., because the requested records do not qualify as *records* in a *system of records*) but the requester is a person asking for access to records about himself or herself, the records custodian must also evaluate the request under the FOIA's disclosure provisions (see 4-4). This is the case even if the request does not cite the FOIA.

c. *Individual.* Any citizen of the United States or alien lawfully admitted for permanent residence. An *individual* does not include the following:

(1) An entity.

(2) A deceased person who qualified as an *individual* prior to death.

(3) An interested party of a deceased person who qualified as an *individual* prior to death when the interested party is inquiring about the existence of or requesting records about the deceased person solely on the basis of his or her status as such an interested party (the interested party does not succeed to the deceased person's Privacy Act notification or access rights). Those interested parties include, but are not limited to, the following:

(a) The executor or administrator of the deceased person's estate.

(b) The deceased person's surviving family members.

Note: While an interested party may not "inherit" or succeed to a deceased individual's Privacy Act rights, the interested party may nevertheless be given access to records under some circumstances. If the interested party claims a legal right to access records, consult your Area Law Office. In addition, in some instances, an interested party may have a right to disclosure of requested records about the deceased person under the FOIA's disclosure provisions (see 4-4). Regarding FOIA Exemption 6, be aware that deceased individuals have a significantly diminished privacy interest in information subject to disclosure (see 4-4.24.2.6).

The following may act on behalf of an *individual*, even without the express consent of an *individual*:

(1) A parent of a minor who is an *individual*.

(2) The legal guardian of an *individual* who has been declared incompetent due to physical or mental incapacity or age by a court of competent jurisdiction.

d. *Maintain.* Maintain, collect, use, or disseminate.

e. *Record.* Any item, collection, or grouping of information that meets all of the following requirements:

(1) Is about an *individual* (including, but not limited to, his or her education, financial transactions, medical history, criminal history, or employment history).

(2) Is *maintained* by the Postal Service.

(3) Contains the *individual's* name or the identifying number, symbol, or other identifying particular assigned to the *individual*, such as a fingerprint, voice print, or photograph.

f. *System of Records*.

(1) *General.* A group of any *records* under the Postal Service's control from which information is retrieved by the *individual's* name or by some number, symbol, or other identifying particular assigned to the *individual*. The Postal Service's systems of records that it has identified under the Privacy Act are set forth in the Appendix.

(2) *Emails.* Emails in the Postal Service's email archive system do not qualify as *records* in a *system of records* (they are not retrieved by the *individual's* name or identifying particular).

(3) *Uncirculated Personal Notes.* Uncirculated personal notes kept by a Postal Service employee about an *individual* do not qualify as a *record* in a *system of records*.

g. *Contractor-Developed or -Operated System.* When the Postal Service contracts for the operation by or on behalf of the Postal Service of a system of records to accomplish a Postal Service function and that system meets the definition in paragraph f., the Privacy Act's notification and access provisions in 4-3 apply to that system.

4-3.2.3 Determining Sufficiency of Form of Request

The records custodian must deny a notification or access request that is not in writing if it is required to be in writing pursuant to the procedures for a requester to make a notification or access request available at *http://about.usps.com/who-we-are/foia/welcome.htm*.

4-3.2.4 Determining Sufficiency of Content of Request

A notification or access request must contain a sufficiently detailed description of the records/system of records inquired about or requested to enable the records custodian to conduct a search for responsive records with a reasonable amount of effort. A notification or access request may not be denied for lack of a sufficient description until the records custodian has given the requester a reasonable amount of time to provide a sufficient description (see 4-3.2.12.b).

4-3.2.5 Verifying Requester's Identity for Access Request

The records custodian must verify the identity of a requester who has submitted an access request to the extent necessary to ensure that the requester is the person he or she represents himself or herself to be. As

appropriate under the circumstances of the access request, the requester may be required to comply with one of the following identification verification methods:

a. *Certification of Identity.* Provision of a completed *Certification of Identity*. A template certification of identity is available at *http://about.usps.com/who-we-are/foia/welcome.htm*.

b. *Official Photo Identification.* Provision of an official photo identification, which includes, but is not limited to, the following:

   (1) A valid driver's license.

   (2) An unexpired passport.

   (3) An unexpired federal government-issued employee identification card.

c. *Privacy Waiver*. Provision of a completed *Privacy Waiver* if the records pertain to another individual available at *http://about.usps.com/who-we-are/foia/welcome.htm*.

An access request may not be denied for lack of sufficient identity verification until the records custodian has given the requester a reasonable amount of time to provide sufficient identity verification (see 4-3.2.12.b).

4-3.2.6 Searching for Responsive Records

If a notification or access request has not been resolved in some other manner, the records custodian must conduct a search of all of the records in the relevant system of records as described in the applicable system of records notice in the Appendix to locate records that are responsive to the request. The records custodian must notify the requester to the extent that no responsive records are found.

4-3.2.7 Determining Whether Records Responsive to Access Request Are Also About Someone Other Than the Requester

To the extent records responsive to an access request are also about someone other than the requester (e.g., records regarding selection for a position), the requester is not provided access to them under the Privacy Act's access provisions in 4-3.2. Instead, the records custodian must determine whether their disclosure to the requester is appropriate under the Privacy Act's external third-party disclosure provisions (e.g., the other person has requested or consented in writing to disclosure to the requester) (see 4-3.3.3) or the FOIA's disclosure provisions (see 4-4).

4-3.2.8 Considering Postal Reorganization Act Exemptions for an Access Request

The records custodian must consider the extent to which records responsive to an access request are exempt from such access under the Postal Reorganization Act (PRA) exemptions described in Exhibit 4-3.2.9. To the extent the responsive records are so exempt, the records custodian may deny the request on that basis, but must also consider the extent to which responsive records exempt from access under the PRA exemptions are also exempt from access under the Privacy Act exemptions (see 4-3.2.9). To the

extent the responsive records are not exempt from access under the PRA exemptions, the records custodian must consider the extent to which they are exempt from access under the Privacy Act exemptions (see 4-3.2.9).

Exhibit 4-3.2.8
Table of Postal Reorganization Act Exemptions

PRA Exemption	What is Exempt
39 U.S.C. 410(c)(1)	The name or address, past or present, of any Postal Service customer, *except* that the name and address of a specifically identified Postal Service customer is disclosed to the general public, upon request, in limited circumstances (see 4-2.2.1).
39 U.S.C. 410(c)(2)	Information of a commercial nature, including trade secrets, whether or not obtained from a person outside the Postal Service, which under good business practice would not be publicly disclosed.
39 U.S.C. 410(c)(3)	Information prepared for use in connection with the negotiation of collective bargaining agreements under 39 U.S.C. Chapter 12, or minutes of, or notes kept during, negotiating sessions conducted under such chapter.
39 U.S.C. 410(c)(4)	Information prepared in connection with proceedings under 39 U.S.C. Chapter 36 relating to rates, classification, and service changes.
39 U.S.C. 410(c)(5)	Reports and memoranda of consultants or independent contractors, except to the extent that they would be required to be disclosed if prepared within the Postal Service.
39 U.S.C. 410(c)(6)	Investigatory files, whether or not considered closed, compiled for law enforcement purposes, *except* to the extent available by law to a party other than the Postal Service. It is Postal Service policy to ordinarily make records compiled for law enforcement purposes available to the general public, upon request, unless the disclosure is covered by FOIA Exemption 7 (see 4-4.24.2.7).

PRA Exemption	What is Exempt
39 U.S.C. 412	Prohibits the disclosure of mailing lists or other lists of names or addresses, past or present, of Postal Service customers or other persons to the public by any means for any purpose, except as specifically authorized by law. In response to a proper FOIA request, the Postal Service may, to the extent required by law, provide a listing of Postal Service employees working at a particular Postal Service facility. See 39 CFR 265.14(e). Regarding Privacy Act requests, the Postal Service may release a list of names and addresses of individuals pursuant to a written request by, or with the prior written consent of, each individual whose name and address is contained in such list, provided that such names and addresses are derived from records maintained by the Postal Service in a system of records as defined by the Privacy Act. See 39 CFR 266.3(b)(3)(iv). See 39 CFR 266.3(b)(3) for other exceptions not related to the FOIA or the Privacy Act.

4-3.2.9 Considering Privacy Act Exemptions

a. *Notification Request.* The records custodian must consider the extent to which records responsive to a notification request are exempt from such notification under the Privacy Act exemptions described in Exhibit 4-3.2.9. To the extent the responsive records are so exempt, the records custodian may deny the request.

b. *Access Request.* To the extent records responsive to an access request are not exempt from such access under the PRA exemptions (see 4-3.2.8), the records custodian must consider the extent to which they are exempt from such access under the Privacy Act exemptions described in Exhibit 4-3.2.9.

(1) *Not Covered Under PRA or Privacy Act Exemptions.* To the extent records responsive to an access request are not exempt from such access under either the PRA exemptions or the Privacy Act exemptions, the records custodian must provide access to the requester (if the other conditions in 4-3 are met).

(2) *Not Covered Under PRA Exemptions But Covered Under Privacy Act Exemptions – Further Evaluation Under the FOIA.* To the extent records responsive to an access request are not exempt from such access under the PRA exemptions, but are exempt from such access under the Privacy Act exemptions, the records custodian must also evaluate whether the responsive records must be disclosed under the FOIA's disclosure provisions (see 4-4). This is the case even if the request does not cite the FOIA.

Exhibit 4-3.2.9
Table of Privacy Act Exemptions

Privacy Act Exemption	What is Exempt
5 U.S.C. 552a(d)(5)	Information that was compiled in reasonable anticipation of a civil action or proceeding. (Applies only to access requests.)
5 U.S.C. 552a(j) Certain criminal law enforcement systems of records.	As identified in the portions of 39 CFR 266.8 and the Appendix invoking 5 U.S.C. 552a(j).
5 U.S.C. 552a(k) Includes, but is not limited to, systems of records that consist of the following: 1. Certain investigatory material compiled for law enforcement purposes (5 U.S.C. 552a(k)(2)). 2. Certain investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualification for federal civilian employment or access to classified information (5 U.S.C. 552a(k)(5)). 3. Certain testing or examination material used solely to determine individual qualification for appointment or promotion in the federal service (5 U.S.C. 552a(k)(6)).	As identified in the portions of 39 CFR 266.8 and the Appendix invoking 5 U.S.C. 552a(k). However, the requester must be provided notification of or access to responsive records that otherwise would be exempt under the portions of 39 CFR 266.8 and the Appendix invoking 5 U.S.C. 552a(k)(2) if the requester is denied any right, privilege, or benefit that he or she would otherwise be entitled to by federal law, or for which he or she would otherwise be eligible, as a result of the maintenance of the responsive records, *except* to the extent that the disclosure would reveal the identity of a source who furnished information to the U.S. Government under either of the following: 1. An express promise that the source's identity would be held in confidence. 2. An implied promise made before the effective date of the Privacy Act that the source's identity would be held in confidence.

4-3.2.10 Handling Medical or Psychological Records Responsive to an Access Request

The records custodian must not provide to the requester medical or psychological records about the requester responsive to an access request (including those received from the Department of Veterans Affairs, Public Health Service, or Office of Workers' Compensation Programs) if in the medical officer's judgment such access could have an adverse effect upon the requester. If the medical officer makes that determination, the medical officer instead transmits the responsive medical or psychological records to

a medical doctor named by the requester, if any. In such cases, an accounting of the disclosure to the medical doctor named by the requester must be kept (see 4-3.5).

4-3.2.11 Assessing and Collecting Fees for Access Request

In response to an access request, the records custodian must provide the requester, at no charge, with hard copies of the first 100 pages of the first copy requested of the responsive records if the requester seeks hard copies of the responsive records. The requester is charged $.15 per page for each other page copied by the records custodian in hard copy. The records custodian must collect the total duplication fee before providing the copies to the requester and deposit the fee in Account Identifier Code (AIC) 127.

4-3.2.12 Responding to the Requester

a. *Acknowledgment of Request.* The records custodian must date stamp the notification or access request (if in a form that permits date stamping) and notify the requester of its receipt no later than 10 business days (excluding weekends and Postal Service holidays) after receipt by the Postal Service, unless the records custodian provides some other response to the requester as provided for in 4-3.2 within that time period.

b. *Notification of Deficiency and Opportunity to Respond.*

(1) *Notification Request.* The records custodian must notify the requester as soon as practical of any deficiency in the sufficiency of the content of a notification request and give the requester a reasonable amount of time to provide a sufficiently detailed description of the records/system of records inquiry (see 4-3.2.4).

(2) *Access Request.* The records custodian must notify the requester as soon as practical of any deficiency in the sufficiency of the content of an access request and give the requester a reasonable amount of time to provide a sufficiently detailed description of the requested records/system of records inquiry (see 4-3.2.4). The records custodian must also notify an access requester as soon as practical of any deficiency in identity verification and give the requester a reasonable amount of time to provide sufficient identity verification (see 4-3.2.5).

c. *Notification of Duplication Fees.* The records custodian must notify the requester as soon as practical of any duplication fees that will be charged with respect to the Postal Service's making requested hard copies of records responsive to an access request.

d. *Time Period for Other Actions.* The records custodian must take the other actions described in 4-3.2 as soon as practical.

e. Response to Requester.

(1) The response to the requester with respect to a notification or access request must be in writing, signed by the records custodian, and sent to the requester by Certified Mail, return receipt requested. If there are records responsive to an access

request that will be made available to the requester for in-person inspection, the records custodian must follow the procedures in paragraph f.

(2) If applicable, the records custodian must provide copies of records responsive to an access request in the form specified by the requester, if feasible (including hard copy or electronic format (e.g., on a disc or thumb drive)). Appropriate security measures must be taken to encrypt and otherwise protect copies provided in electronic format.

(3) If the records custodian has made an adverse determination with respect to an access request (which includes, but is not limited to, a denial of the access request based on a Postal Reorganization Act or Privacy Act exemption or the determination that no responsive records exist), the response must state the reasons for the adverse determination.

(4) If the records custodian has made an adverse determination with respect to a notification or access request, the response must contain the following notification to the requester of his or her administrative appeal rights:

"You have the right to appeal this response in writing sent by mail to the General Counsel, U.S. Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101 and postmarked no later than 90 calendar days after the date of this letter. Your letter of appeal must include, as applicable:

(1) A copy of your original written request, or a reasonable description of the records/system of records of or to which you sought notification or access if your request was not in writing;

(2) A copy of this letter;

(3) Copies of any other correspondence relating to your request;

(4) A statement of the Postal Service's action or failure to act that you are appealing;

(5) A statement of the reasons why you believe the Postal Service's action or failure to act was erroneous; and

(6) A statement of the relief you seek."

f. *Providing In-Person Inspection of Records Responsive to Access Request.* If the requester asks to conduct an in-person inspection of records responsive to an access request, the records custodian must follow these procedures:

(1) The records custodian must notify the requester of the time, date, and location of the inspection, which ordinarily occurs during regular business hours at the facility where the responsive records are kept, but may occur at some other time or location reasonable under the circumstances of the request. If feasible, the records custodian must accommodate the requester's

preferred location, date, and time of inspection. A Postal Service employee must inspect/copy responsive records on his or her own time, *except* as provided for under collective bargaining agreements.

(2) Before permitting the inspection to begin, the records custodian must conduct any necessary identity verification (see 4-3.2.5).

(3) The records custodian must permit the requester to manually record the contents of the responsive records.

(4) The records custodian must be present to observe the requester's inspection of the responsive records.

(5) If, at the conclusion of the inspection, the requester asks for the records custodian to provide copies of the responsive records, such copies must be furnished in the manner provided in 4-3.2.11, 4-3.2.12.c., and 4-3.2.12.e.((2)).

(6) The records custodian may make available to the requester a user-paid copying machine to make hard copies of the responsive records, beyond the hard copies of the first 100 pages of the first copy of the responsive records, which are provided to the requester at no charge (see 4-3.2.11).

(7) The records custodian must permit the requester to have a person of his or her choosing accompany the requester to aid in the inspection (and, if applicable, the manual recording or copying of the responsive records if the requester submits a signed statement authorizing the person to do so) and discussion of the responsive records in the accompanying person's presence.

(8) At the conclusion of the inspection, the records custodian must ask the requester to sign a statement that he or she has inspected the responsive records and include a description of the responsive records. If the requester refuses to sign the statement, the records custodian must note the time, date, and location of the inspection and include a description of the responsive records in the administrative file, which the records custodian maintains relating to the request (see 4-3.2.13).

g. *OPFs and eOPFs.*

(1) *Current Employees.* A current Postal Service employee who is requesting access to his or her electronic Official Personnel Folder (eOPF) should be advised of the option available to the employee to obtain direct access to his or her eOPF (viewing, printing, and, in most cases, requesting a copy) through the Postal Service's *LiteBlue* website (*https://liteblue.usps.gov*). If the employee does not choose that option, or is not eligible to obtain a copy of his or her eOPF through the *LiteBlue* website, the records custodian must respond to the employee's access request in accordance with the procedures in 4-3.2.

(2) *Former Employees.* A former Postal Service employee who is seeking access to his or her eOPF stored at the National

Personnel Records Center (NPRC) (part of the National Archives and Records Administration) or to his or her Official Personnel Folder (OPF) stored at the NPRC that was not converted to an eOPF must be advised of the option available to the former employee to request access to his or her eOPF or OPF directly from the NPRC through the procedures described at *https://www.archives.gov/st-louis/civilian-personnel*. If the former employee does not choose that option, he or she must submit a request for access to his or her eOPF or OPF to the final district Human Resources office or the Human Resources Shared Services Center. The request must receive a response in accordance with the procedures in 4-3.2. The Postal Service official must request the OPF from the NPRC in accordance with the procedures at *https://www.archives.gov/st-louis/civilian-personnel/federal-agencies.html*. The OPF may be retained for a maximum of 30 days after providing access to the requester in case there is a further need for it. Thereafter, the OPF must be returned to the NPRC by Registered Mail.

h. *NACIs.* Requesters who seek access to the results of their National Agency Check with Inquiries (NACI) conducted by the Office of Personnel Management (OPM) must be advised to request such access directly from OPM in accordance with the procedures at *https://www.opm.gov/investigations/freedom-of-information-and-privacy-act-requests/*.

4-3.2.13 Creating and Retaining the Administrative File

a. *Creating the Administrative File.* The records custodian must create an administrative file that memorializes how the notification or access request was processed, including, but not limited to, the following documentation:

(1) All documents pertaining to the request and response, including, but not limited to, the following:

(a) The notification or access request, if in writing, or a description of the records/system of records inquired about or requested, if the request was not in writing.

(b) The final written response sent to the requester.

(c) Any other written correspondence between the Postal Service and the requester.

(2) Adequate documentation of the steps taken in conducting the search for responsive records, if any.

(3) If applicable, the notes of the time, date, and location of the requester's in-person inspection of the responsive records and description of those responsive records if the requester refuses to sign a statement containing that information (see 4-3.2.12.f.((8))).

(4) To the extent not provided in paragraphs (1) – (3), documentation of the records responsive to the notification or access request, if

any, and which records the requester was or was not provided notification of or access to, and the reasons.

b. *Retaining the Administrative File.* The records custodian must retain the administrative file for a period of 7 years from the end of the fiscal year in which the final written response on the notification or access request was sent to the requester.

4-3.2.14 Preserving the Responsive Records

The records custodian may not dispose of the records response to a notification or access request while they are the subject of the pending notification or access request, or an administrative appeal or Privacy Act litigation relating to the request.

4-3.3 Responding to Request by Third Party for Disclosure of Records About an Individual Under the Privacy Act

4-3.3.1 Determining Qualification as a Covered Individual, Record, System of Records, Person, and Agency

a. *General.* The definitions in 4-3.2.2 apply with respect to the records custodian's determination whether disclosure may or must be made under the Privacy Act to a *person* or *agency* of *records* about (another) *individual* in a Postal Service *system of records*. Since an *individual* does not include a deceased person who qualified as an *individual* prior to death (see 4-3.2.2.c), disclosure to a *person* or *agency* of any records about a deceased person is not prohibited under the Privacy Act (but may be protected from disclosure under the FOIA's disclosure provisions (see 4-4)).

b. *Person.* An individual, partnership, corporation, association, or public or private organization other than an *agency*.

c. *Agency.* An executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the United States Government (including the Executive Office of the President), and any independent regulatory agency.

4-3.3.2 Making Internal Disclosures

The records custodian may make disclosure to a Postal Service employee or employee of a Postal Service contractor when the employee has a need for the records in the performance of his or her Postal Service duties.

4-3.3.3 Making External Disclosures

a. *Providing Public Name and Address Information About Specifically Identified Customers.* The records custodian must provide to an external person or agency the name or address information available to the general public about a specifically identified Postal Service customer discussed in 4-2.2.1.

b. *Providing Public Information About Employees.* The records custodian must provide to an external person or agency information available to the general public about Postal Service employees discussed in 4-2.2.2.

c. *Disclosing Non-Public Separation Information About Former Employees to Prospective Employers.* The records custodian may disclose to a former Postal Service employee's prospective employer the following information to the extent provided in 39 CFR 266.3(b)(5) and 5-2:

(1) Date of separation from the Postal Service.

(2) Reason for separation from the Postal Service (limited to retired, resigned, or separated).

d. *Disclosing Records at the Individual's Request or Consent.* If all of the conditions below are met, the records custodian may disclose records to an external person or agency if the individual whom the responsive records are about requests or consents, in writing, to the disclosure. Under these circumstances, the request is processed as if the individual had made an access request, *except* no administrative appeal rights are provided (see 4-3.2).

(1) *Determining Sufficiency of Individual's Request or Consent.* The individual's written request or consent must be given through a completed *Privacy Waiver and Authorization for Disclosure to a Third Party* available at *http://about.usps.com/who-we-are/foia/welcome.htm*. The authorization must be dated no earlier than one year prior to the date the Postal Service receives it and must contain a sufficiently detailed description of the requested records or system of records to enable the records custodian to conduct a search for responsive records.

(2) *Verifying Identities.* Prior to disclosure, the records custodian must verify the individual's and the external person's or agency representative's identities to the extent necessary to ensure that they are who they represent themselves to be. As appropriate under the circumstances, they may be required to comply with one or both of the following identification verification methods:

(a) *Certification of Identity.* Provision of a completed *Certification of Identity* available at *http://about.usps.com/who-we-are/foia/welcome.htm*.

(b) *Official Photo Identification.* Provision of an official photo identification, which includes, but is not limited to, the following:

(i) A valid driver's license.

(ii) An unexpired passport.

(iii) An unexpired federal government-issued employee identification card.

e. *Disclosing Records Pursuant to a Privacy Act-Authorized Disclosure Category.* The records custodian may or must, as applicable, make disclosure to an external person or agency if the disclosure is covered

under one of the Privacy Act's authorized disclosure categories (5 U.S.C. 552a(b)(2) - (12)) described in the Appendix. These include, but are not limited to, the following:

(1) *Required Under the FOIA (5 U.S.C. 552a(b)(2)).* The records custodian **must** make a disclosure if required under the FOIA's disclosure provisions (see 4-4).

(2) *Routine Use (5 U.S.C. 552a(b)(3)).* The records custodian **may** make a disclosure for a routine use provided for in the relevant system of records notice in the Appendix.

(3) *Pursuant to an Order of a Court of Competent Jurisdiction (5 U.S.C. 552a(b)(11)).* The records custodian **must** make a disclosure pursuant to an order of a court of competent jurisdiction to the extent provided in 39 CFR 265.11, 39 CFR 265.12, and 39 CFR 265.13, *except* to the extent that the responsive records are exempt from such disclosure under the Postal Reorganization Act exemptions (see Exhibit 4-3.2.8). The records custodian must consult with his or her legal office upon receipt of a court order requiring disclosure of records. If the order is a matter of public record, the records custodian must make reasonable efforts to notify the individual whom the records are about of their disclosure pursuant to the order, with such notification occurring prior to the disclosure, if feasible.

4-3.3.4 Validating Records Before Making Certain External Disclosures

Before disclosure to an external person of records about another individual in a system of records under 4-3.3, the records custodian must make reasonable efforts to ensure that the disclosed records are accurate, complete, timely, and relevant for Postal Service purposes. This requirement does not apply to disclosure to an external person under the Privacy Act-authorized disclosure category relating to the FOIA (see 4-3.3.3.e(1)), or disclosure to an agency.

4-3.3.5 Notification to Certain External Third Parties of Correction of Records or Notation of Dispute

If the Postal Service makes a correction of or a notation of dispute on records (see 3-6) for which an accounting of disclosures has been or will be made, the records custodian must provide the external person or agency to whom the disclosure was or will be made with the following information, as applicable:

a. Notification that the records have been corrected.

b. A copy of the individual's statement of dispute concerning the records and, if the records custodian deems appropriate, a copy of a concise statement of the Postal Service's reasons for not making the individual's requested amendment to the records.

4-3.4 Administrative Appeals Relating to Notification and Access Requests Under the Privacy Act

4-3.4.1 Responsibility for Deciding Appeal

The Postal Service General Counsel (or designee) is responsible for deciding an administrative appeal by a requester of an adverse determination or failure to act by a Postal Service or Postal Inspection Service records custodian regarding a notification or access request (see 4-3.2). The General Counsel of the Office of Inspector General (OIG) decides administrative appeals by requesters of adverse determinations or failures to act by OIG records custodians regarding notification or access requests.

4-3.4.2 Form and Content of Appeal

a. *Form.* The appeal must be in writing and sent by mail to the following:

GENERAL COUNSEL
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1101

b. *Content.* The letter of appeal must include the following information, as applicable:

(1) A copy of the original written request, or a reasonable description of the records or system of records to which the requester sought notification or access, if the request was not in writing.

(2) A copy of the adverse determination letter.

(3) Copies of any other correspondence relating to the request.

(4) A statement of the Postal Service's action or failure to act that the requester is appealing.

(5) A statement of the reasons why the requester believes the Postal Service's action or failure to act was erroneous.

(6) A statement of the relief the requester seeks.

4-3.4.3 Time Period for Filing Appeal

An appeal is timely filed if it is postmarked in the following timeframe, as applicable:

a. No later than 90 calendar days after the date of the adverse determination letter.

b. No later than 90 calendar days after the date of the request, if the appeal is from a failure of the Postal Service to act on the request.

The General Counsel (or designee) may, within his or her discretion, consider a late appeal.

4-3.4.4 Form and Content of Appeal Decision

The decision of the General Counsel (or designee) must be in writing and contain the following information if the decision upholds the records custodian's adverse determination in whole or part:

a. A statement of the reasons for the affirmance.

b. The requester's statutory right to file a lawsuit.

4-3.4.5 No Adjudication if Privacy Act Suit Filed

An appeal ordinarily will not be adjudicated by the General Counsel (or designee) if the notification or access request becomes the subject of Privacy Act litigation.

4-3.4.6 Final Decision on Issues Appealed

The decision of the General Counsel (or designee) constitutes the Postal Service's final decision on the issues appealed.

4-3.5 Accounting for Disclosures to External Third Parties Under the Privacy Act

4-3.5.1 Keeping Accounting of Disclosures

A records custodian must keep an accurate accounting of each disclosure to an external person or agency of records about an individual in a system of records (see 4-3.3.3), except if the disclosed records are available to the general public (see 4-2).

A records custodian must keep an accounting of a disclosure even if the disclosure was made to the external person or agency at the request or consent of the individual to whom the disclosed records pertain (see 4-3.3.3.e).

An accounting of a disclosure is not kept under either of the following conditions:

a. Disclosure was to the individual to whom the disclosed records pertain (see 4-3.2).

b. Disclosure was to a Postal Service employee or employee of a Postal Service contractor because the employee needed the disclosed records in the performance of his or her Postal Service duties (see 4-3.3.2).

4-3.5.2 Preparing Accounting of Disclosure Record

a. *General. Except* as provided in paragraph b., the records custodian may keep an accounting of a disclosure in hard copy or electronic form and it may consist of a memorandum to the file (see suggested format in Exhibit 4-3.5), a copy of the correspondence transmitting the disclosed records, or a log or other listing that must show the following information:

(1) The date, nature (e.g., employee accident file), and purpose (e.g., legal proceeding) of the disclosure.

(2) The name and address of the external person or agency to whom the disclosure was made.

b. *OPFs and eOPFs.* PS Form 6100-B, *OPF Disclosure Accounting Form*, must be used to account for a disclosure to a law enforcement official of records in a hard copy Official Personnel Folder (OPF) or electronic Official Personnel Folder (eOPF). PS Form 6100-A, *OPF Disclosure Accounting Form*, must be used to account for all other disclosures of

records in a hard copy OPF or eOPF. In lieu of those forms, a system-generated accounting may be used for disclosure from an eOPF.

c. *Collective Bargaining Agents. Except* for disclosures from a hard copy OPF or eOPF, PS Form 6105, *Disclosure of Information About Employees to Collective Bargaining Agents*, must be used to account for disclosures to collective bargaining agents.

d. *Postal Inspection Service.* IS Form 2099, *Inspection Service Disclosure Record*, may be used to account for disclosure of Postal Inspection Service investigative records.

Exhibit 4-3.5
Suggested Format for Memo Documenting External Disclosure of Records

Record of External Disclosure of Records About an Individual From a

System of Records in Compliance with the Privacy Act (5 U.S.C. 552a(c))

Date of disclosure: _____

Disclosed records pertain to: _____ [name of individual]

Disclosed to: _____ [name and address of third party]

Records disclosed: _____ [state, summarize, or otherwise identify]

Source of disclosed records: _____ [no. and name of system of records]

Purpose of disclosure: _____

Authority for disclosure: _____ [Privacy Act section; no. of routine use; identification of individual's written request or consent]

4-3.5.3 Filing and Retention of Accounting of Disclosure Record

a. *Filing.* The accounting of disclosure records must be filed, cross-indexed, or otherwise associated with the disclosed records so that a complete accounting of their disclosure can be constructed, if necessary.

b. *Retention Period.* The accounting of disclosure records must be retained for at least 5 years after the date of the disclosure, or for the life of the disclosed records, whichever is longer.

4-3.5.4 Request for Accounting of Disclosures and Response

a. *Request. Except* as provided in paragraph b., an individual may request an accounting of the disclosure to external persons or agencies of records about the individual in a system of records for which an accounting is required to be kept (see 4-3.5.1). The individual must submit the request to the records custodian, and the request must clearly identify the requester and the records/system of records for which the requester seeks an accounting of disclosures. However, a request for an accounting of disclosures made pursuant to a computer matching program must be submitted to the manager of the Privacy and Records Management Office at the address provided in 1-4.2.5.

b. Response.

(1) *General. Except* as provided in paragraph (2), the records custodian must take one of the following actions no later than 30 business days (excluding weekends and Postal Service holidays) after receipt of a proper request for an accounting of disclosures:

(a) Notify the requester that no relevant disclosures have been made.

(b) Provide the requester with an accounting of the relevant disclosures that have been made.

(2) *Certain External Disclosures Made for Criminal or Civil Law Enforcement Activity.* The records custodian must not provide to the requester an accounting of any disclosures that have been made under the Privacy Act-authorized disclosure category relating to certain disclosures made to other agencies or instrumentalities of governmental jurisdictions within or under the control of the United States for a criminal or civil law enforcement activity (5 U.S.C. 552a(b)(7)) (see 4-3.3.3.e).

4-4 Responding to Requests Under the Freedom of Information Act

4-4.1 Records Required by FOIA to be Made Available to the Public

The procedures in 4-4 do not apply to records maintained in the Postal Service's public and/or electronic reading rooms required by the FOIA to be made available to the general public (see 4-2.1.2). A requester who requests such records must be directed to the public and electronic reading rooms.

4-4.2 Assigning FOIA Tracking Number to and Acknowledgment of Request

For each request that cannot be fully processed within 10 working days (i.e., excluding weekends and Postal Service holidays) of receipt by the Postal Service, the appropriate FOIA requester service center must take the following actions:

a. *FOIA Tracking Number.* Assign the request a tracking number from the Postal Service's FOIA tracking system, which is used in managing the request. The FOIA tracking number must be referenced on all communications sent to the requester about the request.

b. *Acknowledgment of Request.* Notify the requester in writing of the receipt of the request and include the tracking number assigned to the request.

4-4.3 Responsibility for Responding to a Request Under the FOIA

Ordinarily, it is the responsibility of the records custodian (or designee) to respond to an initial request under the FOIA in accordance with the procedures in 4-4. However, in some cases, a FOIA requester service center responds to a request in accordance with the procedures in 4-4. For the purpose of 4-4, "records custodian" means any Postal Service employee who responds to a request under the FOIA. A FOIA requester service center must promptly forward a misdirected request to the appropriate records custodian for response, and notify the requester of the referral.

4-4.4 Evaluating First Under the Privacy Act a Request for Disclosure to the Requester of His or Her Records

When a requester requests the disclosure of records about himself or herself, the records custodian must first evaluate the request under the Privacy Act's access provisions (see 4-3.2). This is the case even if the request does not cite the Privacy Act. This also applies to a proper request by a third party to access records about an individual at the individual's request or consent (see 4-3.3.3.e). As provided in 4-3.2 (see 4-3.2.2.b and 4-3.2.9.b), the records custodian must also, in some scenarios, evaluate a request for disclosure to the requester of records about himself or herself under the FOIA's disclosure provisions in 4-4. This procedure provides the requester with the greatest access to records pertaining to the requester.

Note: A requester's access to records about himself or herself under the FOIA is different than under the Privacy Act. A requester may qualify as a *person* under the FOIA (broader definition) (see 4-3.5.c) but not as an *individual* under the Privacy Act (narrower definition) (see 4-3.2.2.c). In addition, the requested records may qualify as *records* under the FOIA (broader definition) (see 4-4.5.d) but not qualify as *records* about the requester in a Postal Service *system of records* under the Privacy Act (narrower definition) (see 4-3.2.2.e). Further, the FOIA exclusions/ exemptions (see 4-4.22 and 4-4.24) are different than the Privacy Act exemptions (see 4-3.2.9), although in some cases the exemptions are similar (but not identical).

4-4.5 Determining Qualification as a Covered Person and Record

a. *General.* In order for a request to be further considered under the FOIA, the requester must qualify as a *person*, and the requested records must qualify as *record*s.

b. *Agency.* Any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the United States Government (including the Executive Office of the President), and any independent regulatory agency.

c. *Person.* An individual, partnership, corporation, association, or public or private partnership. *Person* does not include:

(1) An agency;

(2) A fugitive from justice who is requesting *records* or information relating to his or her fugitive status.

(3) An individual who has waived his or her FOIA disclosure rights by plea agreement and is requesting *records* or information concerning any waived subject.

d. *Record*.

(1) *General.* Information that meets the following requirements:

(a) Was created or obtained by the Postal Service in any format (including, but not limited to, paper documents or information in electronic form or format).

(b) Is in the Postal Service's control at the time of the request (including, but not limited to, records maintained for the Postal Service by an entity under contract with the Postal Service for the purpose of records management).

(2) *Emails.* Emails in the Postal Service's email archive system qualify as *records*.

(3) *Uncirculated Personal Notes.* Uncirculated personal notes kept by a Postal Service employee do not qualify as a *record*.

4-4.6 Determining Sufficiency of Form of Request

All FOIA requests must be made in writing.

4-4.7 Determining Whether a Request Asks for Disclosure of Records

A valid request under the FOIA must ask for the disclosure of records. Generally, a request that asks the Postal Service to answer questions, as opposed to release records, is not a request for the disclosure of records. However, records custodians must interpret requests liberally and consider the request to be a request under the FOIA for a disclosure of records. Records custodians should respond accordingly, if the request is in the form of a question, yet reasonably describes the records that the requester is seeking. See 4-4.9.a.

4-4.8 Determining Whether a Request Provides the Requester's Full Name and Mailing Address

A request must provide the requester's full name and mailing address. A request may not be denied for lack of provision of the requester's full name and mailing address until the records custodian has given the requester 30 calendar days to provide his or her full name and address.

4-4.9 Determining Sufficiency of Content of Request

a. *Reasonably Described Records.* A request must reasonably describe the records requested, i.e., the request must contain a sufficiently detailed description of the requested records to enable the records custodian to conduct a search for responsive records with a reasonable amount of effort. A request does not necessarily fail to meet this requirement just because it is burdensome. A request may not be denied for lack of sufficient description until the records custodian has given the requester 30 calendar days to provide a sufficient description. The custodian should explain how the Postal Service's records pertinent to the request are filed, indexed, or grouped so that the requester understands how to narrow the request.

b. *Request That Does Not Cite the FOIA.* A request for records that does not cite the FOIA, but follows all other requirements in 39 CFR 265.3 for making a FOIA request, must be processed in accordance with 4-4. A request for information that does not cite FOIA or follow any of the requirements in 39 CFR 265.3 for making a FOIA request must not be treated as a FOIA request; there is no obligation under the FOIA to respond to such requests. A media request for information that does not cite the FOIA or follow any of the requirements in 39 CFR 265.3 for making a FOIA request must be forwarded to Corporate Communications. See 5-6.

c. *Broad Email Search Requests.* See 4-4.14 for issues concerning broad requests for all emails on a particular topic.

4-4.10 Requesting Additional Information About the Request

The records custodian may ask the requester once for additional information needed to respond to the request. During the period the records custodian is awaiting receipt of the additional information, the time period for the records custodian to respond to the request (see 4-4.14) is tolled (stopped), i.e., the records custodian is not required to consider the request further during that period.

4-4.11 Verifying the Requester's Identity

The records custodian must verify the identity of a requester who has requested records about himself or herself to the extent necessary to ensure that the requester is the person he or she represents himself or herself to be. See 4-3.2.5 for identity verification procedures.

During the period the records custodian is awaiting receipt of the identity verification information, the time period for the records custodian to respond to the request (see 4-4.14) is tolled (stopped), i.e., the records custodian is not required to consider the request further during that period.

4-4.12 Determining Whether to Neither Confirm Nor Deny the Existence of Records

In some circumstances, a FOIA request can be narrowly targeted so that by its very terms, merely acknowledging the existence of responsive records would cause harm. The records custodian may have to neither confirm nor deny the existence of any responsive records. In such cases, the records custodian is not required to conduct a search for records responsive to a request or perform an analysis to identify segregable portions of such records to the extent that it is appropriate to provide a response to the requester neither confirming nor denying the existence of responsive records. Such a response is appropriate when merely acknowledging the existence of responsive records would itself cause the harm one of the FOIAs exemptions is designed to prevent, most commonly one of the following:

a. FOIA Exemption 1 (records properly classified under executive order to be kept secret in national defense or foreign policy interest).

b. FOIA Exemption 6 (personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy).

c. FOIA Exemption 7(C) (information or records compiled for law enforcement purposes the disclosure of which would constitute an unwarranted invasion of personal privacy).

d. FOIA Exemption 7(E) (information or records compiled for law enforcement disclosure of which would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law).

The U.S. Department of Justice's *Guide to the Freedom of Information Act* available at *http://www.justice.gov/oip/foia_guide09.htm* includes guidance regarding when it is appropriate to provide a response to a requester neither confirming nor denying the existence of responsive records.

4-4.13 Assessment and Collection of Fees

a. *General/Consultation of FOIA Regulations.* If the request is not otherwise resolved, the records custodian must assess and collect from the requester all allowable fees incurred by the Postal Service in responding to the request. Title 39 CFR 265.9 of the Postal Service's FOIA regulations outlines how a records custodian may charge fees. While general guidance concerning fee issues is provided here, this guidance is meant to supplement a review of 39 CFR 265.9. Records custodians must *always* review 39 CFR 265.9 of the Postal Service's FOIA regulations carefully *before* proceeding with a request, as some requests may require advance payment or the records custodian may find that it is necessary to ask the requester additional information in order to clarify issues regarding fees. Title 39 CFR 265.9 also provides guidance in determining whether a requester qualifies for a waiver of

fees, if he or she so requests one. The referring FOIA RSC or the Privacy and Records Management Office may serve as resources to assist with fee questions.

b. *Categories of Requesters and Types of Fees Charged.* Generally, FOIA provides for several categories of requesters for purposes of charging fees: commercial use requesters, representatives of the news media, educational and noncommercial scientific institutions, and all others. Commercial use requesters may be charged for fees incurred in searching and reviewing records, as well as duplication fees. Representatives of the news media and educational or scientific institutions may be charged only for duplication fees. All other requesters may be charged for search and duplication fees. Additional special costs may apply depending on the particular circumstances of the request. Title 39 CFR 265.9 includes guidance regarding categorizing requesters, as well as the particular amount that a requester may be charged. For all categories of requesters besides commercial use requesters, the first 100 pages of duplication and 2 hours of search time is free of charge.

c. *Representatives of the News Media.* If a requester asserts that he or she must be categorized as a representative of the news media, the requester must demonstrate several things. First, the requester must demonstrate that he or she, or the news entity represented, gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. Some examples include television networks, radio stations, publishers of periodicals, and websites that disseminate news and make their products available through a variety of means to the general public. Disseminating solely on the internet may qualify. However, merely making the information received available to the public (or others), as opposed to disseminating the information, is not sufficient to qualify a requester for placement in this fee category. Furthermore, the request must be in furtherance of the entity or individual's news gathering function for the request to qualify for this category. A "freelance" journalist must demonstrate a solid basis for expecting publication through a news media entity to be considered as a representative of the news media, for example by presenting a publishing contract or his or her past publication record. If the requester does not provide sufficient information to determine if he or she qualifies as a representative of the news media, send a letter to the requester asking for additional information with a response deadline of 10 business days. It is the requester's obligation to demonstrate that he or she meets the requirements to be considered a representative of the news media.

d. *More Information Required and Time Limits.* If it is necessary to ask the requester for further information in order to clarify issues regarding fee assessment, then the time period for the records custodian to respond to the request is tolled while the records custodian awaits that information (see 4-4.14). In other words, the records custodian is not required to consider the request further during that period.

e. *Fees Not Assessed.* The Postal Service does not charge for responding to requests for records if fees do not exceed $25 or for requests for address information as described in 5-2.

f. *Advance Notice.* The custodian must notify the requester as soon as practicable if the estimated processing cost is expected to exceed $25, unless:

(1) The request specifies that whatever cost is involved is acceptable or is acceptable up to a specified amount that covers estimated costs; or

(2) Payment of all fees in excess of $25 has been waived (see 39 CFR 265.9 for fee waiver provisions).

The custodian must briefly describe the basis for the estimated cost and may offer the requester the opportunity to revise the request to reduce the cost. If the custodian does not hear from the requester within 20 working days, he or she will assume the requester is no longer interested in pursuing the request. Whenever practical, the custodian should advise the requester in writing that he or she is closing the file since a response was not received.

g. *Advance Payment.* Advance payment may be required:

(1) When the estimated fees are likely to exceed $250. The custodian may require an advance payment of an amount up to the full estimated charge before commencing work on the request.

(2) When a requester has previously failed to pay a fee within 30 days of billing. In such instances, the requester is *required* to pay the full amount owed and make an advance payment of the estimated fees.

When advance payment is required, the time for response does not run between the date the notice requiring advance payment is sent and the date payment is received. If the custodian does not hear from the requester within 20 working days, he or she will assume that the requester is no longer interested in pursuing the request. Whenever practical, the custodian must advise the requester in writing that he or she is closing the file since a response was not received.

h. *Consequences of Failing to Meet Statutory Time Limits.* Unless unusual circumstances apply, when a component fails to comply with FOIA's time limits for responding to a request (see 4-4.14) it may not charge search fees or, for requests where no search fees may be charged (requests from educational institutions, noncommercial scientific institutions, or representatives of the news media), may not charge duplication fees.

i. *Accounting for Fees.* Custodians must account for fees as follows:

(1) For fees received at Post Office installations, deposit fees received as Postal Service funds. Record the amounts collected by entries to Account Identifier Code (AIC) 198, Freedom of Information Fees.

(2) For fees received at non-Post Office installations, forward fees for deposit to the following:

DISBURSING OFFICER
U.S. POSTAL SERVICE
EAGAN ACCOUNTING SERVICE CENTER
2825 LONE OAK PARKWAY
EAGAN, MN 55121

Specify general ledger account 43388, Freedom of Information Fees, as the account for the amounts collected.

j. *Searches for Emails and Other Electronic Databases.* If the request involves a search for emails or other electronic databases by the USPS Information Catalog Program (ICP), then ICP must be asked to provide a fee estimate before proceeding with the search (see 4-4.18).

k. *Appeal Rights Provided.* Because fee waiver denials are considered adverse determinations, requesters must be provided with appeal rights (see 4-4.26.c and 4-4.28).

4-4.14 Time Limits

The law requires that the Postal Service respond to requests within 20 working days from the date the Postal Service receives the request. If the request is referred to a records custodian by a FOIA RSC, the referring FOIA RSC will supply the records custodian with the request's due date. Within 10 business days of receiving a referral of a request from a FOIA RSC, the records custodian must confirm by email that his or her office is processing the request and provide the name of the person(s) within his or her department that are handling the request.

4-4.15 Time Extensions

a. *General.* The statutory time limit for responding to a request may be extended with written notice to the requester under certain unusual circumstances. This includes:

(1) The need to search for and collect records from a facility other than the one processing the request;

(2) The need to search for, collect, and examine a voluminous amount of records; or

(3) The need to consult with another agency, or two or more components of the Postal Service, having a substantial interest in the record(s) (see 4-4.19).

If the request is referred from a FOIA RSC, the records custodian must contact the referring FOIA RSC as soon as possible if it appears that an extension may be necessary and warranted under the circumstances detailed above.

b. *Notification to Requester.* Whenever the statutory time limit for processing a request cannot be met because of unusual circumstances, as defined above, the Postal Service shall, before the

expiration of the 20-day period to respond, notify the requester in writing of:

(1) The unusual circumstances involved; and

(2) The date by which the Postal Service expects to complete the processing of the request.

c. *Extensions Exceeding 10 Working Days.* If the extension exceeds 10 working days, the Postal Service must:

(1) Provide the requester with an opportunity to modify the request or arrange an alternative time period for processing;

(2) Alert the requester to the availability of the Office of Government Information Services to provide dispute resolution services; and

(3) Make available its designated FOIA contact and its FOIA Public Liaison.

d. *Voluntary Extensions.* By mutual agreement and within the initial 20-day response period, the custodian and the requester may establish a different response period. Confirm agreement with the requester in writing. For requests referred from a FOIA RSC, consult with the FOIA RSC prior to arranging a voluntary extension of a response time.

4-4.16 Multitrack Processing

Unless expedited processing is granted (see 4-4.17), the Postal Service places each request in a simple or complex track based on the amount of work and time involved in processing the request. Within each track, the Postal Service generally responds to requests in the order that they are received. Several factors are considered in assigning a request to a particular track, including:

a. Whether the request involves voluminous documents;

b. The complexity of the material;

c. Whether the request involves record searches at multiple facilities or locations;

d. Whether the request requires consultation among components of the Postal Service or other agencies; and

e. The number of open requests submitted by the same requester.

4-4.17 Expedited Processing

The Postal Service may grant expedited processing of requests under certain circumstances. See 39 CFR 265.5(c). This determination may be made by the records custodian or the referring FOIA RSC as appropriate. The requester must be notified of the determination within 10 calendar days and provided with appeal procedures, if expedited processing is denied. See 4-4.28. If expedited processing is granted, the request is processed as soon as practicable. Records custodians will be notified whether a request has been granted expedited processing upon referral from the FOIA RSC.

4-4.18 Searching for Responsive Records

The records custodian must conduct a search for records that are responsive to a request. The search must be done in the most efficient and least expensive manner. The records custodian must make reasonable efforts to locate the requested records, including records in paper format; in storage; and in electronic format, except when such efforts would significantly interfere with the operation of a Postal Service electronic information system.

a. *Cut-Off Date of Search*. The records custodian ordinarily must search for responsive records in the Postal Service's possession as of the date the search begins, unless the request identifies a specific date or date range for the requested records. The records custodian may extend the cut-off date for the search in his or her discretion. If the cut-off date for the search is extended, the records custodian must notify the requester of that date.

b. *Searches for Emails.* A request for "any and all emails" about a broad subject matter is typically not considered to meet the reasonable description standard (see 4-4.9). If a request for email records is insufficient, the responding component must ask the requester to narrow the request based on one or more of the following criteria: (1) keyword search terms, (2) name of the sender(s) or recipient(s), or (3) a definitive time period. Unless a request is limited to a desktop search, the responding component must complete PS Form 3002, *Data Request*, and either mail the completed data request under confidential cover or email it to the following:

INFORMATION CATALOG PROGRAM
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260
EMAIL: *ICPMAIL@USPS.GOV*

c. *Searches of Other Electronic Databases.* Unless a request is limited to a desktop search or the information is readily accessible by desktop by a Postal Service employee authorized through eAccess to access the data, complete PS Form 3002, *Data Request*, and either mail the completed data request under confidential cover or email it to the following:

INFORMATION CATALOG PROGRAM
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260
EMAIL: *ICPMAIL@USPS.GOV*

d. *Questions*. Postal Service employees may contact ICP at 202-268-4437 with questions.

e. *Documentation of Search.* The records custodian must maintain adequate documentation of his or her steps in conducting the search, including an accounting of search and review time, in order to properly calculate fees or to respond to administrative appeals.

4-4.19 Referral to or Consultation or Coordination With Another Postal Service Component or Agency

a. *General.* To the extent the responsive records originated from another Postal Service component or *agency* (see 4-4.5.b), the records custodian must refer the responsive records or information to the other Postal Service component or *agency* to process under the FOIA's disclosure provisions and provide a direct response to the requester, *except* if one of the exceptions in paragraph b. is met. The three Postal Service components are the Postal Service, the Postal Inspection Service, and the Postal Service Office of Inspector General. The records custodian must identify responsive records appropriate for referral to another Postal Service component or *agency* as soon as practical during the course of processing the request. For requests referred from a FOIA RSC, consult the referring FOIA RSC as soon as possible when you believe that records may require consultation or referral.

b. *Exceptions to Use of Referral Procedures.* The records custodian **may not** use the referral procedures under the following circumstances:

(1) *Originator of Records is Not Subject to the FOIA.* If the originator of the responsive records is not subject to the FOIA, the records custodian must follow the consultation process with respect to the responsive records (see 4-4.20). Only a federal entity that qualifies as an *agency* (see 4-4.5.b) is subject to the FOIA, which does not include the United States Congress, United States courts, state governmental entities, private entities, or individuals.

(2) *Agreement to Use Consultation Procedures.* If there is joint agreement with the originating Postal Service component or other agency that the responsive records should be handled by way of a consultation instead of a referral, the records custodian must follow the consultation procedures (see 4-4.20) instead of the referral procedures.

(3) *Conditions for Coordinating a Response Are Met:* If the conditions for coordinating a response with the other Postal Service component or agency are met (see 4-4.20), the records custodian must follow the coordination procedures instead of the referral procedures.

c. *Procedures for Making a Referral.* If referral to another Postal Service component or agency is appropriate, the records custodian must follow these procedures:

(1) Determine whether the referring Postal Service component has an interest in whether the responsive records are disclosed to the requester.

(2) Send the following to the originating Postal Service component or agency as soon as practical:

(a) A copy of the request.

(b) A copy of the responsive records.

(c) A cover memorandum stating the following:

(i) The FOIA tracking number the Postal Service assigned to the request.

(ii) The date the request was received by the Postal Service.

(iii) If applicable, the recommendation of the referring Postal Service component as to whether the responsive records must be disclosed to the requester.

(3) Notify the requester that a referral of responsive records has been made for disclosure decision and direct response to the requester, provide the name of the Postal Service component or other agency to which the referral was directed, and include that component's or agency's FOIA contact information.

(4) Maintain a copy of the responsive records being referred and the cover memorandum accompanying the referral.

4-4.20 Coordinating Response With Another Postal Service Component or Agency

a. *General.* Instead of following the referral procedures (see 4-4.19) at all or at first, the records custodian must follow the procedures in paragraphs b. and c., as applicable, when both of the following conditions are met:

(1) The responsive records are one of the following:

(a) Law enforcement records that originated from another Postal Service component that is a law enforcement component (i.e., the Postal Inspection Service or the Postal Service Office of Inspector General) or from another agency that is a law enforcement agency.

(b) Classified records that originated from an agency that is a member of the intelligence community.

(2) Following the referral procedures may invade a person's personal privacy or damage national security interests by revealing involvement of the originating Postal Service component or agency in a matter because that involvement has not been publicly acknowledged.

b. *Determining Whether Records May be Referred.* If the conditions in paragraph a. are met, the records custodian must take the following actions:

(1) Inquire of the originating Postal Service component or agency whether that component's or agency's involvement in the matter can be publicly acknowledged without invading the person's personal privacy or damaging national security interests. Provide to the component or agency a copy of the request and copies of the responsive records as necessary to facilitate this inquiry process.

(2) If the originating Postal Service component or agency indicates that its involvement in the matter can be publicly disclosed without invading the person's personal privacy or damaging national security interests, the referral procedures must be followed (see 4-4.19).

(3) If the originating Postal Service component or agency indicates that its involvement in the matter cannot be publicly disclosed without invading the person's personal privacy or damaging national security interests, the coordination procedures in paragraph c. must be followed.

c. *Coordinating Response With Originating Component or Agency.* If coordination with the originating Postal Service component or agency is appropriate, the records custodian must take the following actions:

(1) Obtain the views of the originating Postal Service component or agency as to how to respond to the requester with respect to disclosure of the responsive records.

(2) Fully process the request under standard procedures, incorporating into the response letter sent to the requester the views of the originating Postal Service component or agency as to how to respond to the requester with respect to the disclosure of the responsive records.

4-4.21 Procedures Upon Receipt of a Consultation from Another Agency

Whenever the Postal Service receives a consultation request from another agency, it must respond as promptly as practical to facilitate the other agency's ability to finalize its response to the request. Upon receipt of a consultation, custodians must take the following steps:

a. Contact the Privacy and Records Management Office to ensure a FOIA tracking number is assigned to the consultation request.

b. Promptly provide the Postal Service's views on the disclosability of the contents of the records to the agency seeking the consultation.

4-4.22 Considering FOIA Exclusions

The records custodian must consider the extent to which records responsive to a request are excluded from the FOIA under the FOIA exclusions applicable to the Postal Service described in Exhibit 4-4.22. To the extent the responsive records or information are so excluded, the records custodian may notify the requester that there are no records responsive to the request.

The U.S. Department of Justice's *Guide to the Freedom of Information Act* available at *http://www.justice.gov/oip/foia_guide09.htm* includes guidance regarding application of the FOIA exclusions.

Exhibit 4-4.22
Table of FOIA Exclusions

FOIA Exclusion	What is Excluded
5 U.S.C. 552(c)(1)	During only such time as all of the following conditions are met, the responsive records or information may be treated as not subject to the FOIA: a. A request involves access to records described in FOIA Exemption 7(A) (see 4-4.24.2.7). b. The investigation or proceeding involves a possible violation of criminal law. c. There is reason to believe both of the following: (1) The subject of the investigation or proceeding is not aware of its pendency, and (2) The disclosure of the existence of the responsive records could reasonably be expected to interfere with enforcement proceedings.
5 U.S.C. 552(c)(2)	The responsive records or information may be treated as not subject to the FOIA if all of the following conditions are met: 1. A criminal law enforcement agency (i.e., the Postal Inspection Service or the Postal Service Office of Inspector General) maintains an informant's records under the informant's name or personal identifier, 2. A third party requests those informant's records according to the informant's name or personal identifier, and 3. The informant's status has not been officially confirmed.

4-4.23 Considering Postal Reorganization Act Exemptions

To the extent the responsive records are not excluded from the FOIA under a FOIA exclusion (see 4-4.22), the records custodian must consider the extent to which they are exempt from disclosure under the Postal Reorganization Act (PRA) exemptions described in Exhibit 4-4.23. To the extent the records are so exempt, the records custodian may deny the request. If the request is denied under a PRA exemption, the records custodian must also deny it under FOIA Exemption 3 as the PRA exemption statutes are both an independent source of exemption and exempting statutes under FOIA Exemption 3 (see 4-4.24.2.3; also see 4-4.26 for information to include in a response).

Exhibit 4-4.23
Table of Postal Reorganization Act Exemptions

PRA Exemption	What is Exempt
39 U.S.C. 410(c)(1)	The name or address, past or present, of any Postal Service customer, *except* that the name and address of a specifically identified Postal Service customer is disclosed to the general public upon request in limited circumstances (see 4-2.2.1).
39 U.S.C. 410(c)(2)	Information of a commercial nature, including trade secrets, whether or not they are obtained from a person outside the Postal Service, which under good business practice would not be publicly disclosed.
39 U.S.C. 410(c)(3)	Information prepared for use in connection with the negotiation of collective bargaining agreements under 39 U.S.C. Chapter 12 or minutes of, or notes kept during, negotiating sessions conducted under such chapter.
39 U.S.C. 410(c)(4)	Information prepared in connection with proceedings under 39 U.S.C. Chapter 36 relating to rates, classification, and service changes.
39 U.S.C. 410(c)(5)	Reports and memoranda of consultants or independent contractors, except to the extent that they would be required to be disclosed, if prepared within the Postal Service.
39 U.S.C. 410(c)(6)	Investigatory files, whether or not considered closed, compiled for law enforcement purposes, *except* to the extent available by law to a party other than the Postal Service. ***Note:*** However, it is the Postal Service's policy to ordinarily make records or information compiled for law enforcement purposes available to the general public upon request unless the disclosure is covered by FOIA Exemption 7 (see 4-4.24.2.7).
39 U.S.C. 412	Prohibits the disclosure of mailing lists or other lists of names or addresses, past or present, of Postal Service customers or other persons to the public by any means for any purpose, except as specifically authorized by law. In response to a proper FOIA request, the Postal Service may, to the extent required by law, provide a listing of Postal Service employees working at a particular Postal Service facility. See 39 CFR 265.14(e). Regarding Privacy Act requests, the Postal Service may release a list of names and addresses of individuals pursuant to a written request by, or with the prior written consent of, each individual whose name and address is contained in such list, provided that such names and addresses are derived from records maintained by the Postal Service in a system of records as defined by the Privacy Act. See 39 CFR 266.3(b)(3)(iv). (See 39 CFR 266.3(b)(3) for other exceptions not related to the FOIA or the Privacy Act.)

4-4.24 Considering FOIA Exemptions

4-4.24.1 General

a. *General.* To the extent the responsive records or information are not exempt from disclosure under a PRA exemption (see 4-4.23), the records custodian must consider whether they are exempt from disclosure under the FOIA exemptions described in 4-4.24.2.1 through 4-4.24.2.9.

The U.S. Department of Justice's *Guide to the Freedom of Information Act* available at *http://www.justice.gov/oip/foia_guide09.htm* includes guidance regarding application of the FOIA exemptions.

b. *Discretionary Disclosures.* A records custodian may, and is encouraged to, disclose records or information that are otherwise exempt from disclosure under a FOIA exemption if such disclosure is not prohibited by law, executive order, or regulation and the disclosure would not cause foreseeable harm covered by a FOIA exemption. Before making such a discretionary disclosure, the custodian must consider the following:

(1) The effect of non-disclosure on the public's right to know about a particular matter.

(2) The effect of disclosure on the right of privacy of any affected individuals. In particular, information covered by Exemption 6 is not appropriate for discretionary disclosure (see 4-4.24.2.6).

(3) The effect of disclosure on the public interest in the economical, efficient, and orderly operation of the nation's mail system.

(4) The effect of disclosure on the security of the mails, Postal Service property, and Postal Service employees.

(5) The age of the document and the sensitivity of its content.

(6) Any other factors that may be relevant under the circumstances.

4-4.24.2 Exemptions

4-4.24.2.1 Exemption 1 — Information Properly Classified Under Executive Order to Be Kept Secret in National Defense or Foreign Policy Interest

Exemption 1 (5 U.S.C. 552(b)(1)) exempts from disclosure records or information that meet both of the following requirements:

a. Are specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy, and

b. Are in fact properly classified pursuant to such executive order.

Classified records in the custody of the Postal Service are managed by the Postal Inspection Service.

4-4.24.2.2 Exemption 2 — Information Related Solely to Agency Internal Personnel Rules and Practices

Exemption 2 (5 U.S.C. 552a(b)(2)) exempts from disclosure records or information related solely to an agency's internal personnel rules and practices.

Exemption 2 covers only records or information that meet both of the following requirements:

a. Concern Human Resources and employee relations (e.g., hiring, selection, placement, and training; policies and procedures governing current employees; employee relations and Human Resources; compensation and benefits; conditions of employment; work rules, disciplinary procedures and appeals, and termination); and

b. Are not of a significant public interest (i.e., the records or information do not shed light on the Postal Service's operations or activities).

The types of records or information covered by Exemption 2 may be appropriate for discretionary disclosure when there is no foreseeable harm in releasing them (see 4-4.24.1.b).

4-4.24.2.3 Exemption 3 — Specifically Exempted Form Disclosure by Another Federal Statute

Exemption 3 (5 U.S.C. 552(b)(3)) exempts from disclosure information that is exempt from disclosure under another federal statute, including the Postal Reorganization Act (39 U.S.C. 410(c) and 412). Exhibit 4-4.24.2.3 lists the statutes and a brief description of the type(s) of information withheld under each statute most frequently relied upon by the Postal Service. Other statutes may apply. When withholding records under Exemption 3, records custodians must cite in the response letter the federal statute relied on to withhold the records.

Exhibit 4-4.24.2.3
Exemption 3 Statutes

Statute	Description
39 U.S.C. 410(c)(1)	Permits the withholding of the name or address, past or present, of any Postal Service customer.
39 U.S.C. 410(c)(2)	Information of a commercial nature, including trade secrets, whether or not obtained from a person outside the Postal Service, which under good business practice would not be disclosed. Such information includes, but is not limited to, the following: ■ Information pertaining to methods of handling valuable Registered Mail. ■ Records of money orders, except as provided in R900 of the *Domestic Mail Manual*. ■ Technical information concerning postage meters and prototypes submitted for Postal Service approval before leasing to mailers. ■ Reports of market surveys conducted by or under contract on the Postal Service's behalf. ■ Records indicating rural carrier lines of travel. ■ Records compiled within the Postal Service, which would be of potential economic benefit to persons or firms in economic competition with the Postal Service. ■ Information that, if publicly disclosed, could materially increase procurement costs. ■ Information that, if publicly disclosed, could compromise testing or examination materials. ■ On request, information of a general nature (e.g., an outline of the geographic area served by a particular rural route, the route numbers and number of boxholders or families on each rural route and highway contract route, and the number of families or businesses served within the total delivery area) may be disclosed. Do not disclose detailed information or use Postal Service route maps for this purpose. A map provided by the requester may be marked with the general information. Disclosure is a matter of local discretion when it is determined that to do so would not interfere with Postal Service operations. ■ Information, including internal guidelines, that, if revealed, would threaten the security and safety of Postal Service operations, facilities, equipment, or employees.
39 U.S.C. 410(c)(3)	Information prepared for use in the negotiation of collective bargaining agreements under 39 U.S.C. Chapter 12 and minutes of notes kept during the negotiating sessions.
39 U.S.C. 410(c)(4)	Information prepared for proceedings under 39 U.S.C. Chapter 36 relating to rates, classification, and service changes.
39 U.S.C. 410(c)(5)	Reports and memoranda of consultants or independent contractors, except to the extent that they would be required to be disclosed if prepared within the Postal Service.
39 U.S.C. 410(c)(6)	Investigatory files, whether or not considered closed, compiled for law enforcement purposes, except to the extent available by law to a party other than the Postal Service.

Statute	Description
39 U.S.C. 412	Prohibits the disclosure of mailing lists or other lists of names or addresses, past or present, of Postal Service customers or other persons to the public by any means for any purpose, except as specifically authorized by law. In response to a proper FOIA request, the Postal Service may, to the extent required by law, provide a listing of Postal Service employees working at a particular Postal Service facility. See 39 CFR 265.14(e). Regarding Privacy Act requests, the Postal Service may release a list of names and addresses of individuals pursuant to a written request by, or with the prior written consent of, each individual whose name and address is contained in such list, provided that such names and addresses are derived from records maintained by the Postal Service in a system of records as defined by the Privacy Act. See 39 CFR 266.3(b)(3)(iv). (See 39 CFR 266.3(b)(3) for other exceptions not related to the FOIA or the Privacy Act.)
18 U.S.C. 1461	Records concerning nonmailable matter.
18 U.S.C. 2510 – 2520	Records relating to wiretap requests and information.
Rule 6(e) of the Federal Rules of Criminal Procedure	Grand jury information.
Section 7(b) of the Inspector General Act of 1978	Confidentiality of employee complaint information.

4-4.24.2.4 Exemption 4 — Trade Secrets and Privileged or Confidential Commercial or Financial Information Obtained by Agency From Any Person

Exemption 4 (5 U.S.C. 552(b)(4)) exempts from disclosure trade secrets and privileged or confidential commercial or financial information obtained by an agency from any person, such as a supplier or customer. The records custodian must follow the procedures in section 5-2c before disclosing third-party business information.

4-4.24.2.5 Exemption 5 — Internal or Interagency Information

Exemption 5 (5 U.S.C. 552(b)(5)) exempts from disclosure interagency or internal memoranda or letters that would not be available by law to a private party in litigation with the Postal Service. This incorporates civil discovery privileges, including the deliberative process privilege, attorney-client privilege, and attorney work-product privilege. The deliberative process privilege permits withholding of pre-decisional, deliberative (nonfactual) information such as drafts, internal proposals, estimates, statements of opinion, analysis, advice, and recommendations of agency employees to be used in the decision-making process of an agency. The types of records covered by Exemption 5 may be appropriate for discretionary disclosure when there is no foreseeable harm in releasing them (see 4-4.24.1.b). However, **always** consult a Postal Service attorney concerning information that may be classified as attorney-client or attorney work-product privileged, such as any communications to or from a Postal Service attorney.

4-4.24.2.6 Exemption 6 — Personal, Medical, and Similar Information the Disclosure of Which Would Constitute a Clearly Unwarranted Invasion of Personal Privacy

Exemption 6 (5 U.S.C. 552(b)(6)) exempts from disclosure personal and medical and similar files, the disclosure of which would be a clearly unwarranted invasion of personal privacy. “File” under Exemption 6 broadly includes actual hard copy files as well as other types of records and bits of information. “Personnel,” “medical,” and “similar” files are similarly interpreted broadly and are not limited to records or information containing only intimate details or highly personal information about an individual, but can encompass many different types of files and information in the possession of the Postal Service that specifically identify an individual.

In determining whether to release records that may be protected by Exemption 6, the custodian must balance the privacy interests of the individuals involved against the public interest, if any, that would be sufficient to outweigh the privacy interests of the individuals involved. For the purposes of Exemption 6, the only public interest to be weighed is the extent to which disclosure would serve the “core purpose” of the FOIA, which is to contribute significantly to public understanding of the operations or activities of the government, or, in other words, to shed light on the conduct of the Postal Service. Additionally, Exemption 6 cannot be invoked to withhold from a requester information pertaining only to himself or herself (see 4-4.4).

Once a custodian has determined that the privacy interest of the individual outweighs any public interest, material covered by Exemption 6 is not appropriate for discretionary disclosure.

4-4.24.2.7 Exemption 7 — Certain Information Compiled for Law Enforcement Purposes

Exemption 7 (5 U.S.C. 552(b)(7)) exempts from disclosure records or information compiled for law enforcement purposes, but only to the extent that the disclosure of such records or information:

a. Exemption 7(A) – could reasonably be expected to interfere with enforcement proceedings.

b. Exemption 7(B) – would deprive a person of a right to a fair trial or impartial adjudication.

c. Exemption 7(C) – could reasonably be expected to constitute an unwarranted invasion of personal privacy.

d. Exemption 7(D) – could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis and, in the case of records or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.

e. Exemption 7(E) – would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

f. Exemption 7(F) – could reasonably be expected to endanger the life or physical safety of any individual.

4-4.24.2.8 Exemption 8 — Information Related to Agency Responsible for Regulation or Supervision of Financial Institutions

Exemption 8 (5 U.S.C. 552(b)(8)) exempts records and information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions and rarely, if ever, applies to Postal Service records or information.

4-4.24.2.9 Exemption 9 — Geological/Geophysical Information and Data Concerning Wells

Exemption 9 (5 U.S.C. 552(b)(8)) exempts geological and geophysical information and data, including maps concerning wells.

4-4.25 Determining Segregable Portions of Records and Marking PRA/FOIA Exemptions

If the records custodian determines that a PRA or a FOIA exemption applies to responsive records, the records custodian must then determine whether there are any non-exempt portions of the records that may be disclosed or, in other words, are reasonably segregable from the exempt portions. If so, the records custodian must delete (redact) only the exempt portions of the records. The amount of information deleted and the PRA/FOIA exemption under which the deletion is made must be indicated on the disclosed portions of the record(s), unless including that information would harm an interest protected by that exemption. If technically feasible, the amount of information deleted and the exemption applied must be indicated at the place in the records where the deletion is made.

4-4.26 Writing the Response

a. *General.* All requests must be responded to in writing. Records custodians may contact their area Law Department with legal questions concerning a response. Records custodians are also encouraged to contact their FOIA coordinator (see Exhibit 4-4.27). Records custodians may also consult the FOIA RSC regarding procedural questions. However, it is the responsibility of the records custodian to draft the response letter.

b. *Grants of Requests.* If a request is granted in whole or in part, a written response must accompany the records that the custodian chooses to release. The response must include a statement notifying the requester of his or her right to seek assistance from the appropriate FOIA Public Liaison (see 4-4.26.e). A list of FOIA public liaisons can be found here: *https://about.usps.com/who-we-are/foia/service-centers.htm*. In

addition, the letter must inform the requester of any fees charged (see 4-4.13). Any responsive non-exempt records withheld on the basis of non-payment of fees must be released promptly upon the requester's payment of fees.

c. *Adverse Determinations, Decisions Included*. If a records custodian makes an adverse determination on any aspect of a request, he or she must notify the requester of that determination in writing. Many determinations regarding a request may constitute an adverse determination, including a determination that:

(1) The requested record is exempt from disclosure in whole or in part (see 4-4.23 and 4-4.24);

(2) The request does not reasonably describe the records sought (see 4-4.9);

(3) The information requested is not a record subject to the FOIA (see 4-4.5.d);

(4) The requested record does not exist, cannot be located, or has been destroyed; or

(5) The requested record is not readily reproducible in the form or format sought by the requester.

Denials of fee waivers (see 4-4.13 and 39 CFR 265.9) and denials of requests for expedited processing (see 4-4.17) also constitute adverse determinations.

d. *Adverse Determinations, Response Letter*. Regarding a request or a portion of a request for which a records custodian makes an adverse determination, the accompanying response letter must include:

(1) The name and title or position of the person responsible for the denial;

(2) A brief statement of the reasons for the denial, including any exemption applied by the component in denying the request and how the exemption applies to the withheld material (see 4-4.23 and 4-4.24);

(3) A statement that the denial may be appealed and a description of the requirements for filing such an appeal (see 4-4.28 and 39 CFR 265.8);

(4) A statement notifying the requester of his or her right to seek dispute resolution services from the FOIA Public Liaison or the Office of Government Information Services;

(5) An estimate of the volume of any records or information withheld, such as the number of pages or some other reasonable form of estimation, *unless:*

(a) The volume of withheld records is otherwise indicated by redactions marked on disclosed records; or

(b) Providing an estimate would harm any interest protected by an applicable exemption. For example, if an individual requests a third party's disciplinary records, but the

records are withheld under Exemption 6, it would hurt the protection of the third party's privacy interests to state that a disciplinary file does exist but was withheld (see 4-4.12).

e. *Sample Appeal Language.* Adverse determinations must include appeal rights language, such as:

"If you are not satisfied with the response to your request, you may file an administrative appeal by writing to the General Counsel, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101, or by email at *FOIAAppeal@usps.gov*. Your appeal must be postmarked or, in the case of electronic submissions, submitted within 90 calendar days of the date of this letter. The letter of appeal must include, as applicable:

(1) A copy of the request, of any notification of denial or other action, and of any other related correspondence;

(2) The FOIA tracking number assigned to the request;

(3) A statement of the action, or failure to act, from which the appeal is taken;

(4) A statement identifying the specific redactions to responsive records that the requester is challenging;

(5) A statement of the relief sought; and

(6) A statement of the reasons why the requester believes the action or failure to act is erroneous.

For further assistance and to discuss any aspect of your request, you may contact any of the following (include name, title, and contact information):

- Name of agency official,
- Records custodian, or
- FOIA Coordinator that processed your request.

Include one or more of the following FOIA Public Liaison's contact information based on the type of records requested:

U.S. Postal Service

USPS HQ FOIA Requester Service Center — FOIA requests for Postal Service Headquarters controlled records including contracts, building leases, and other real estate transactions; or employee listings must be directed to:

PRIVACY AND RECORDS MANAGEMENT OFFICE
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW RM 1P830
WASHINGTON, DC 20260-1101
TELEPHONE: 202-268-2608
FAX: 202-268-5353
FOIA PUBLIC LIAISON: JANE EYRE
TELEPHONE: 202-268-2608

Field FOIA Requester Service Center — FOIA requests for Postal Service records controlled by area offices, district offices, Post Offices, or other field operations facilities must be directed to:

FOIA REQUESTER SERVICE CENTER
ST. LOUIS GENERAL LAW SERVICE CENTER
U.S. POSTAL SERVICE
1720 MARKET STREET RM 2400
ST. LOUIS, MO 63155-9948
TELEPHONE: 314-345-5894
FAX: 650-578-4956
FOIA PUBLIC LIAISON: LINDA CRUMP

U.S. Postal Inspection Service

OFFICE OF COUNSEL
U.S. POSTAL INSPECTION SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON, DC 20260-1101
TELEPHONE: 202-268-7004
FAX: 202-268-4538
FOIA PUBLIC LIAISON: TAMMY WARNER

f. *Sample OGIS Language.* In addition to contact information for the FOIA Public Liaison, adverse determinations must include a statement regarding the requester's right to seek dispute resolution services from OGIS, such as:

"You may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA meditation services that they offer. OGIS may be contacted in any of the following ways:

OFFICE OF GOVERNMENT INFORMATION SERVICES
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
8610 ADELPHI ROAD – OGIS
COLLEGE PARK, MD 20740-6001
EMAIL: *OGIS@NARA.GOV*
FAX: 202-741-5769
TELEPHONE: 202-741-5770
TOLL FREE: 877-684-6448

4-4.27 Documentation and Preservation of Records

a. *Administrative File.* All records custodians **must** maintain an administrative file documenting how they responded to a FOIA request. The administrative file must contain the following:

(1) A Completed PS Form 8170 (see 4-4.27.b);

(2) A copy of any responsive records, including any responsive records that were withheld in full based on a FOIA exemption (see 4-4.23 and 4-4.24) and any records released in full to the requester;

(3) If records were released to the requester with redactions, a copy of the redacted records and a copy of the unredacted records;

(4) All correspondence pertaining to each request;

(5) Clear documentation of the steps taken in conducting a records search; and

(6) An accounting of search time and review time used in calculating fees.

b. *Completing PS Form 8170.* Records custodians must consult with their FOIA Coordinator when completing PS Form 8170. Use Exhibit 4-4.27 to locate the appropriate FOIA coordinator. A list of current FOIA coordinators for each location may be found on the Privacy and Records Blue site: *http://blue.usps.gov/uspslaw/Privacy/records/foia_resources.htm*.

Exhibit 4-4.27
FOIA Coordinators

Records Custodians	Where to Send Reports
Located in area offices.	FOIA coordinator in the area office.
Located in processing and distribution center offices.	FOIA coordinator in the performance cluster.
Located in customer service and sales district offices.	FOIA coordinator in the performance cluster.
Located at Headquarters and in Headquarters field units.	Headquarters department FOIA coordinator.
Postmasters	FOIA coordinator in the performance cluster.

c. *Forwarding Completed Documents.* The Records Custodian must, upon consultation with the FOIA Coordinator, forward the completed PS Form 8170 and a copy of the response to the FOIA RSC.

d. *Retention Period.* The Records Custodian must retain the administrative file, including all of the items detailed in 4-4.27.a. for a period of 7 years from the end of the fiscal year in which the final response occurs.

e. *Administrative Appeals and Litigation Holds.* If the requester appeals a response (see 4-4.28), the FOIA RSC will request that the Records Custodian forward a copy of the administrative file to the FOIA RSC. If the request becomes the subject of litigation, the Records Custodian will receive a litigation hold notice from the Area Law Department handling the litigation. In the event of a litigation hold, the litigation hold controls the retention period for any documents within its scope, including but not limited to the administrative file.

4-4.28 Administrative Appeals

a. *General*. Adverse decisions (see 4-4.26.c.) of the Postal Service or the Postal Inspection Service may be appealed to the General Counsel.

b. *Time Limit*. To be considered timely, the appeal must be postmarked or, in the case of electronic submissions, transmitted within 90 calendar days after the date of the response, or within a reasonable time if the appeal is from a failure of the custodian to act. The General Counsel may, in his or her discretion, consider late appeals.

c. *Form and Manner of Submission.* The appeal must be in writing and must be addressed to the General Counsel, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101 or sent by email to *FOIAAppeal@usps.gov*.

d. *Required Appeal Elements*. The appeal must include, as applicable:

(1) A copy of the request, of any notification of denial or other action, and of any other related correspondence;

(2) The FOIA tracking number assigned to the request;

(3) A statement of the action, or failure to act, from which the appeal is taken;

(4) A statement identifying the specific redactions to responsive records that the requester is challenging;

(5) A statement of the relief sought; and

(6) A statement of the reasons why the requester believes the action or failure to act is erroneous.

e. *Final Decision.* The decision of the General Counsel constitutes the final decision of the Postal Service.

4-4.29 After the Final Decision

a. *Outcomes on Appeal.* On appeal, the General Counsel may affirm, affirm in part, reverse, or reverse in part the initial FOIA response of a records custodian. The General Counsel may also remand the request in whole or in part to the records custodian for further processing. In this instance, the requester may appeal from the additional response of the records custodian following remand.

Right to Review. A decision that upholds a component's adverse determination in whole or in part will contain a statement that identifies the reasons for the affirmance, including any FOIA exemptions applied. The decision will provide the requester with notification of the statutory right to file a lawsuit and will inform the requester of the mediation services offered by the Office of Government Information Services of the National Archives and Records Administration as a non-exclusive alternative to litigation.

5 Requests for Special Categories of Records

5-1 General

The following guidance applies when responding to requests for certain categories of records that are frequently requested and may involve special processing rules. This chapter concerns requests for six special categories of records:

- Employee or customer records, such as customer name and address data;
- Records requested on behalf of Congress;
- Records subject to litigation;
- Records requested by a Postal Service collective bargaining unit;
- Requests from the news media; and
- Requests for surveys.

5-2 Requests for Employee or Customer Information

a. General.

(1) If requesters seek records about themselves, see 4-3.2 for Privacy Act protected records, as well as 4-4.4 under the FOIA. If a third party requests information about another Postal Service employee or customer at that employee or customer's request or authorization, see 4-3.3.3.e (for Privacy Act records) and 4-4.4 (FOIA). If the requester seeks records about another customer, employee, or other individual and not at that individual's request or consent, then additional privacy rules apply. Subsection 5-2.b. contains some categories of employee and customer information that may be disclosed to third parties in special circumstances. Otherwise, if the information is a Privacy Act record maintained in a system of records (see 4-3.2.2), it may only be released as allowed under the Privacy Act (see 4-3.3). Furthermore, while many Privacy Act systems (see Appendix) allow for disclosure of customer or employee information when *required* by the FOIA (see 4-4), keep in mind that a FOIA exemption, such as Exemption 6, may still protect the

information (see 4-4.24). Even if the information is not subject to the Privacy Act, Exemption 6 (or another FOIA exemption) may bar its disclosure. Finally, nonpublic or confidential information about business customers or the Postal Service should not be disclosed under the FOIA if exempt, such as under the Postal Reorganization Act and/or FOIA Exemptions 3 or 4 (see 4-4.23 and 4-4.24).

b. *Employee Information Subject to Disclosure.* Information other than those categories listed here may only be disclosed under the general rule above; however, you may disclose the following employee information:

(1) *Employment Data.* With the exception of law enforcement personnel, the following data is considered public information: the name, job title, grade, current salary, duty station, and dates of employment of any current or former Postal Service employee. Salary history may not be provided given potential links to performance information and resulting privacy interests.

(2) *Release of Employee Records for Credit or Job* References. Public information about a current or former employee may be given to prospective employers, or to credit bureaus, banks, federal credit unions, and other commercial firms from which an employee is seeking credit. For former employees, prospective employers may also be given the date and reason for an employee's separation from the Postal Service, but the reason for separation must be limited to one of the following terms:

- Retired,
- Resigned, or
- Separated.

Other terms or variations of these terms (e.g., retired — disability) may not be used. If a credit firm or prospective employer requests more information, it must submit a release form signed by the individual (see 4-3.3.3.e for identity verification forms that may be used).

(3) *Employee Listings.* On written request, the Postal Service provides, to the extent required by law, a listing of employees working at a particular Postal Service facility (but not their home addresses, employee identification numbers, or Social Security numbers).

(4) *Verification of Employment or Income.* Employees or verifiers may verify employment or income of current Postal Service employees by calling *The Work Number* at 800-367-5690 or by visiting *www.theworknumber.com*. The requester must use Employer code 12946. The employee will need to set up a salary key if wages need to be verified. The key can only be used once and is good for 30 days only.

c. *Third Party Business Information.* A custodian may only release nonpublic third party business information in accordance with these procedures:

(1) *General.* Under FOIA Exemption 4, any person or entity who submits business information to the Postal Service ("submitter") is entitled to request that the information not be disclosed. The submitter may request that information be withheld:

- When submitting the information, by designating all or part of the information as not releasable (e.g., by marking designated information as privileged or not releasable); or
- In response to notice of a FOIA request.

If information is supplied on a recurring basis, a simplified means of identifying non-releasable information may be agreed upon by the submitter and the custodian. Protective designations expire 10 years after the records were submitted unless the submitter provides a reasonable justification for a longer period. No action is needed by the custodian unless a request for the submitter's information is received.

(2) *Notification*:

(a) *General.* Unless an exception applies, the custodian must notify a submitter within 5 days (excluding weekends and federal holidays) after a FOIA request is received for the submitter's business information if:

- The submitter has designated the information as protected from disclosure; or
- In the opinion of the custodian, or the general counsel in the case of an appeal, disclosure of the information could result in competitive harm to the submitter.

The notification must either describe the exact nature of the business information requested, or provide copies of the records or portions of records containing the business information. The custodian must notify the requester that notice and an opportunity to object are being provided to the submitter.

(b) *Exceptions.* Notification does not need to be made if:

(i) The custodian determines that the information will not be disclosed.

(ii) The information lawfully has been published or has been officially made available to the public by the submitter.

(iii) Disclosure of the information is required by law (other than the FOIA).

(iv) Disclosure of the particular kind of information is required by a Postal Service regulation. In such cases, the custodian must provide advance written

notification to the submitter if the submitter had designated the information as protected.

(3) *Submitter Objections to Disclosure.* The custodian must give the submitter a reasonable time (e.g., 10 working days) to provide a detailed written statement of any objection to disclosure. The objection must specify the grounds for withholding any of the information under any FOIA exemption. Specifically, under FOIA Exemption 4, the submitter must demonstrate why the information is a trade secret, or commercial or financial information that is privileged or confidential. When possible, the objection should be supported by a statement or certification by an officer or authorized representative of the submitter that the information in question is:

- Confidential,
- Has not been disclosed to the public by the submitter, and
- Is not routinely available to the public from other sources.

The objection and any accompanying information may also be subject to disclosure under FOIA.

(4) *Disclosure.* If planning to disclose records over the submitter's objection, the custodian must furnish the submitter a written notice that includes:

(a) A description of the business information to be disclosed.

(b) A statement of the reasons the submitter's objections were not sustained.

(c) The specific date on which disclosure is to occur. The notice of intent to disclose must be provided to the submitter in a reasonable number of days before the specified disclosure date, and the requester must be notified that the notice of intent has been provided to the submitter.

(5) *Nondisclosure.* If the custodian determines that any part of the requested records should not be disclosed, the custodian must notify the requester in writing, and include the right to appeal the decision. See 4-4.26 and 4-4.28. A copy of the letter of denial must also be provided to the submitter in any case in which the submitter had been notified of the request. If a requester brings a lawsuit seeking to compel disclosure of business information, the general counsel or designee must promptly notify the submitter.

d. *Customer Names and Addresses.* The procedures related to the disclosure of customer names and addresses are as follows (see also 39 CFR 265.14):

(1) *Customer or Mailing Lists.* Mailing lists or other lists of names or addresses (past or present) of Postal Service customers or other persons may not be made available to the public by any means or for any purpose except that in response to a proper FOIA request, the Postal Service may, to the extent required by law, provide a listing of Postal Service employees working at a

particular postal facility. See 39 CFR 265.14(e). Regarding Privacy Act requests, the Postal Service may release a list of names and addresses of individuals pursuant to a written request by, or with the prior written consent of, each individual whose name and address is contained in such list, provided that such names and addresses are derived from records maintained by the Postal Service in a system of records as defined by the Privacy Act. See 39 CFR 266.3(b)(3)(iv). (See 39 CFR 266.3(b)(3) for other exceptions not related to the FOIA or the Privacy Act, including when required by the terms of a legally enforceable contract or interagency agreement and subject to a valid non-disclosure agreement.)

(2) *Address Location.* If the location of an address is known, a Postal Service employee may disclose the location or give directions to the address.

(3) *Release of Address Information for Specific Customers*. Upon request, the names and addresses of specifically identified Postal Service customers will be made available only as follows:

(a) *General.* Information relating to boxholders, permanent and temporary change of address, and commercial mail receiving agencies may only be disclosed as permitted by the Privacy Act and routine uses for the applicable system of records. See the Appendix, additional instructions in 5-2d(3)(b), and Exhibit 5-2a, *Address Disclosure Chart*.

(b) *Additional Instructions.* The following additional instructions must be followed relating to requests for change of address or boxholder information.

(i) *General.* Disclosures must be limited to the address of the specific individual about whom information is requested, not other family members or individuals whose name may appear on the change of address form. The address of an individual may be withheld to protect the individual's personal safety. If an individual has filed for a protective order, the address may not be disclosed except pursuant to a court order and on the advice of counsel.

(ii) *To persons serving legal process.* This includes persons empowered by law, the attorney for a part on whose behalf service is to be made, or a party who is acting pro se (the term *pro se* means that a party is self-represented, and is not represented by an attorney). When responding, do not provide a copy of PS Form 3575, *Change of Address Order,* or PS Form 1093, *Application for Post Office Box Service,* to the requester. The USPS does not have a standard form for use when requesting address information. Requesters are encouraged to use the standard format in Exhibit 5-2b. If the requester uses

the standard format on its own letterhead, the standard format must be used in its entirety, and the warning statement and certification must appear immediately before the signature block. If the request lacks any of the required information or a proper signature, the custodian must return it to the requester specifying the deficiency. Requests via facsimile from process servers are acceptable. Each request must specify all of the following information:

1. A certification that the name or address is needed and will be used solely for service of legal process in connection with actual or prospective litigation.
2. A citation to the statute or regulation that empowers the requester to serve process, if the requester is anyone other than a party acting pro se or the attorney for a party for whom service will be made.
3. The names of all known parties to the litigation.
4. The court in which the case has been or will be commenced.
5. The docket or other identifying number, if one has been issued.
6. The capacity in which the individual is to be served (e.g., defendant or witness).

(iii) *To a federal, state,* or local government agency. Address verification is provided to government agencies that provide written certification that the information is needed to perform their duties. Address verification may also extend to a government contractor if its request is submitted on the agency's letterhead and contains a certification signed by a duly authorized agency official that the contractor requires the information to perform official agency business pursuant to the contract with the agency. The contractor's request may also be on its own letterhead if accompanied by the agency certification. Verification means advising the agency as to whether the address provided is one at which mail for that customer is currently being delivered. It does not mean or imply knowledge on the part of the Postal Service about the actual residence of the customer or the actual receipt of mail delivered to that address. Agencies must use the standard format in Exhibit 5-2c when requesting address verification. If the request lacks any of the required information or a proper signature, the custodian must return the request to the agency specifying the deficiency in the

space marked “other.” Requests via facsimile from government agencies are acceptable.

(iv) *For jury service.* The known mailing address of any customer sought for jury service is provided without charge to a court official, such as a judge, court clerk, or jury commissioner, upon prior written request.

Exhibit 5-2a
Address Disclosure Chart

Type of Requester	Disclose Boxholder Information from PS Form 1093, *Application for Post Office Box Service* (Both Business and Personal Use)	Disclose Individual/ Family Change of Address from PS Form 3575	Disclose Business Change of Address	Disclose Commercial Mail Receiving Agency Customer Information from PS Form 1583, *Application for Delivery of Mail Through Agent* (Both Business and Personal Use)
General public	No	No	Yes	No, except for the purpose of identifying a particular address as being that of a Commercial Mail Receiving Agency. Do not furnish copy of form.
Process server	Only if written request includes all of the information in Exhibit 5-2b, including the warning and certification above the signature block. Disclose only the name or address of the boxholder applicant. Do not furnish a copy of the form. Do not disclose the name or address of an individual who has filed a protective court order. See exception.*	Only if written request includes all of the information in Exhibit 5-2b, including the warning and certification above the signature block. Do not furnish a copy of the form. The address of an individual who has filed a protective court order will not be disclosed.	Yes	No, except for the purpose of identifying a particular address as being that of a Commercial Mail Receiving Agency. Do not furnish a copy of the form.
Subpoena or court order	Only if counsel concurs.	Only if counsel concurs.	Yes	Only if counsel concurs.

Type of Requester	Disclose Boxholder Information from PS Form 1093, *Application for Post Office Box Service* (Both Business and Personal Use)	Disclose Individual/ Family Change of Address from PS Form 3575	Disclose Business Change of Address	Disclose Commercial Mail Receiving Agency Customer Information from PS Form 1583, *Application for Delivery of Mail Through Agent* (Both Business and Personal Use)
Criminal law enforcement (applies to government agencies whose function is law enforcement such as local police department, county sheriff, state police, or FBI)	Boxholder name/address and the names of other persons listed as receiving mail on the PS Form 1093 may be disclosed if the agency request is in writing and in compliance with Postal Service certification and signature requirements. A copy of the form may be disclosed if requested by the agency. Do not disclose the name or address of an individual who has filed a protective court order. See exception.*	For written requests from these agencies, follow the instructions for "government agency." For oral requests from these agencies, disclosure pursuant to oral requests through the Inspection Service is permitted, if the Inspection Service has confirmed the information is needed for a criminal investigation.	Yes. Disclosure may be made pursuant to oral requests through the Inspection Service.	No, except for the purpose of identifying a particular address as being that of a Commercial Mail Receiving Agency. Do not furnish a copy of the form. See exception.*
Government agency	Boxholder applicant name/address and the names of other persons listed as receiving mail on PS Form 1093 may be disclosed if the agency request is in writing and in compliance with Postal Service certification and signature requirements. A copy of the form may be disclosed if requested by the agency. Do not disclose the name or address of an individual who has filed a protective court order. See exception.*	Only if written signed request is on letterhead and it is for official purposes. See required format in Exhibit 5-2c. Signatures may be preprinted, rubber stamped, or electronically prepared; letterheads may be computerized. Duplicate envelopes or self-addressed stamped envelopes are not required.	Yes	No, except for the purpose of identifying a particular address as being that of a Commercial Mail Receiving Agency. Do not furnish copy of form. See exception.*

***Exception:** If a protective order has been filed with the postmaster on behalf of an individual or on behalf of a customer of a Commercial Mail Receiving Agency, information from PS Form 1093, Application for Post Office Box or Caller Service, or from PS Form 1583, Application for Delivery of Mail Through Agent, may not be released unless the requester has obtained an order of a court of competent jurisdiction that requires the disclosure in spite of the existence of the protective order. Seek the advice of counsel.*

Exhibit 5-2b
Change of Address or Boxholder Request Format — Process Servers

To: Postmaster Date_____

_____
City, State, ZIP Code

REQUEST FOR CHANGE OF ADDRESS OR BOXHOLDER INFORMATION NEEDED FOR SERVICE OF LEGAL PROCESS

Please furnish the new address or the name and street address (if a boxholder) for the following:

Name:_____

Address:_____

Note: Only one request may be made per completed form. The name and last known address are required for change of address information. The name, if known, and Post Office box address are required for boxholder information

The following information is provided in accordance with 39 CFR 265.14(d). There is no fee for providing boxholder or change of address information.

1. Capacity of requester (e.g., process server, attorney, party representing self):_____
2. Statute or regulation that empowers me to serve process (not required when requester is an attorney or a party acting pro se - except a corporation acting pro se must cite statute):

_____

_____

3. The names of all known parties to the litigation:_____
4. The court in which the case has been or will be heard:_____
5. The docket or other identifying number (a or b must be completed):
   ____ a. Docket or other identifying number: _____
   ____ b. Docket or other identifying number has not been issued.
6. The capacity in which this individual is to be served (e.g., defendant or witness): _____

WARNING

THE SUBMISSION OF FALSE INFORMATION TO OBTAIN AND USE CHANGE OF ADDRESS INFORMATION OR BOXHOLDER INFORMATION FOR ANY PURPOSE OTHER THAN THE SERVICE OF LEGAL PROCESS IN CONNECTION WITH ACTUAL OR PROSPECTIVE LITIGATION COULD RESULT IN CRIMINAL PENALTIES INCLUDING A FINE OF UP TO $10,000 OR IMPRISONMENT OF NOT MORE THAN 5 YEARS, OR BOTH (TITLE 18 U.S.C. SECTION 1001).

I certify that the above information is true and that the address information is needed and will be used solely for service of legal process in conjunction with actual or prospective litigation.

_____ _____
Signature Address

_____ _____
Printed Name City, State, ZIP Code

POST OFFICE USE ONLY

_____No change of address order on file.
_____Moved, left no forwarding address.
_____No such address.

NEW ADDRESS OR BOXHOLDER'S NAME
POSTMARK AND STREET ADDRESS

_____
_____
_____

Exhibit 5-2c
Address Information Request Format — Government Agencies

(AGENCY LETTERHEAD)

To: Postmaster

_____

Agency Control Number: _____

Date: _____

ADDRESS INFORMATION REQUEST

Please furnish this agency with the new address, if available, for the following individual or verify whether the address given below is one at which mail for this individual is currently being delivered. If the following address is a Post Office box, please furnish the street address as recorded on the boxholder's application form.

Name: _____

Last Known Address: _____

I certify that the address information for this individual is required for the performance of this agency's official duties.

_____

(Signature of Agency Official)

_____

(Title)

FOR POST OFFICE USE ONLY

[ ] MAIL IS DELIVERED TO ADDRESS GIVEN

[ ] NOT KNOWN AT ADDRESS GIVEN

[ ] MOVED, LEFT NO FORWARDING ADDRESS

[ ] NO SUCH ADDRESS

[ ] OTHER (SPECIFY):

_____

_____

Agency return address

NEW ADDRESS

_____

_____

BOXHOLDER STREET ADDRESS

_____

_____

Postmark/Date Stamp

5-3 Congressional Requests

For records sought by or on behalf of a Congressional committee or subcommittee that oversees the Postal Service, promptly forward the request to the vice president, Government Relations, for response. Disclosure is the general rule. In most cases, only Executive privilege could justify nondisclosure. Other requests from individual members of Congress, including those made on behalf of a constituent, should be processed under the procedures in Chapter 4. A copy of any such request should be immediately forwarded to the vice president, Government Relations, on an informational basis. A copy of any interim or final responses should also be provided to the vice president, Government Relations, at:

VICE PRESIDENT GOVERNMENT RELATIONS
U.S. POSTAL SERVICE
475 L'ENFANT PLZ SW RM 10804
WASHINGTON, DC 20260

5-4 Records Subject to Litigation

For records sought pursuant to subpoena, court order, summons, or regarding matters that are in litigation or likely to become the subject of litigation, the custodian must immediately advise appropriate Field Legal Counsel. Custodians should contact the General Counsel's office if appropriate legal counsel is unknown. Records may only be released on advice of counsel. Postal Service regulations concerning providing records subject to subpoenas and legal proceedings are contained in 39 CFR 265.11-13.

5-5 Records Requested by Postal Service Unions

Unions may request information under the National Labor Relations Act (NLRA) or FOIA. In addition, certain collective bargaining agreements include a provision that enables unions to request relevant information necessary for collective bargaining or the enforcement, administration, or interpretation of the agreements. These requests are usually labeled "Request for Information" or "Information Requests." Requests made under the NLRA or a collective bargaining agreement should be forwarded to the appropriate Labor Relations office for response. Requests for records that cite the FOIA should be processed under the procedures in Chapter 4, as appropriate. Seek clarification from the requester if a request is not clearly labeled as an Information Request or a FOIA request. Provide a copy of the initial decision and any records released in response to a union's FOIA request to the appropriate district manager for Labor Relations.

5-6 Records Requested by the News Media

Corporate Communications works closely with Postal Service departments to facilitate disclosure of nonexempt information and records to news media requesters. That office strives to handle such requests through the most efficient means possible by helping requesters identify particular records and coordinating with records custodians to determine whether those records are readily disclosable. This approach often results in the satisfaction of such requests for agency records without a formal FOIA request. For members of the news media, the Postal Service has public affairs officers available to address media inquiries across the country. See *http://about.usps.com/news/media-contacts/welcome.htm*.

For FOIA requests concerning a breaking news media inquiry, field offices should immediately provide a copy of any such request to the appropriate Area field manager for Corporate Communications. For headquarters units, contact the manager, Media Relations, at National Headquarters. It is important to make sure that your external communications are accurate and coordinated through Corporate Communications. An advance copy of any interim or final response to the news media should be provided to the appropriate Communications office. Postal Service employees who need additional guidance for handling media inquiries and other communications activities should contact the Corporate Communications office or local communications office. Also, see the Administrative Support Manual, section 332, at *http://blue.usps.gov/cpim/ftp/manuals/asm/asmtc.pdf*.

See 4-4.13.c for information on determining whether an individual requester or entity making a FOIA request may qualify as a “representative of the news media” for purposes of assessing fees.

News media inquiries involving the Inspection Service should be directed to the Inspection Service.

5-7 Requests to Conduct Research or to Survey Postal Service Employees

The Leadership Development and Talent Management Office has responsibility for responding to requests from third parties for permission to conduct surveys of Postal Service employees, or to conduct research about Postal Service operations, policies, or personnel. This does not include requests from Postal Service employees acting in their official capacity, nor does it apply to surveys or research conducted by third parties pursuant to a contract with the Postal Service. Postal Service employees advancing requests in furtherance of their obtaining an academic degree will be deemed to be acting in their official capacity. The benefits the Postal Service is likely to gain from the requester survey or research is balanced against the

disruption of Postal Service activities and protecting the privacy of individuals. Any such requests should be promptly forwarded to:

MANAGER, LEADERSHIP DEVELOPMENT AND
TALENT MANAGEMENT OFFICE
HUMAN RESOURCES
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260

Surveys involving the Inspection Service should be directed to the Inspection Service.

This page intentionally left blank

6 Records Management

6-1 Records Management Policy

6-1.1 General

Postal Service records management is based on best practices, business needs, and legal requirements. The policy applies to all Postal Service employees, business partners and suppliers who create, receive, or maintain records for the Postal Service. Procedures that provide specific instruction on various records management requirements are referenced in this section.

Proper and systematic management of Postal Service records is essential to Postal Service business needs and to assure compliance with applicable laws and regulations. Policy objectives are to:

a. Set standards for the management of records throughout their lifecycle.

b. Facilitate Postal Service compliance with records retention requirements.

c. Ensure that records relevant for ongoing business purposes, or for current or future litigation, investigations or audits are appropriately preserved and reasonably accessible.

d. Safeguard records including third-party records.

e. Reduce inefficiencies in the records management process.

6-1.2 What You Need to Know About Records

What you need to know about records is the following:

a. All records, including e-mails and instant messages, created or received by the Postal Service or its employees are the property of the Postal Service and shall be managed in accordance with this policy and related procedures.

b. Each Postal Service functional area will have a records control schedule that lists its official record categories and sets forth the applicable retention periods (see section 6-3). The Records Office coordinates the development and updates of all records control schedules. Final approval is required by the functional area, the Law Department, Inspection Service, and the Privacy Office. Records must be disposed of at the end of the retention period, unless there is a legal hold requiring preservation of the records.

c. Each Postal Service functional area is responsible for properly designating records, including identifying any vital records (see 6-2) and for safeguarding records in its possession.

6-1.3 Records Safeguards

Appropriate safeguards, such as access restrictions, passwords, records controls, lockable cabinets, or lockable rooms, must be provided to ensure the security and privacy of records in order to protect the interests of the Postal Service, its employees, customers, suppliers, and the general public. (See Handbook AS 805, *Information Security.)*

Information contained in records may be proprietary to a supplier. That information must be managed in accordance with relevant contractual obligations, if any, that the Postal Service may have entered into with that supplier, as well as any applicable laws, including FOIA.

6-2 Records Creation and Designation Guidelines

6-2.1 General

This section sets forth procedures for creating and designating records.

6-2.2 Creating a Record

Records often survive long past their business need and later may be interpreted by people with little or no understanding of their context. When creating a record, use the following steps:

1. Create only those records that are necessary to meet a Postal Service business need.
2. Use clear, accurate, and professional language when creating a record.
3. Take steps to ensure that confidentiality is preserved where appropriate.

6-2.3 Record Designation

Some records warrant special designation and protection. The Postal Service uses four designations for such records: sensitive, critical, classified, and vital.

a. **Sensitivity of records** measures the need to protect the confidentiality and integrity of personal and business information. The three levels in order of decreasing sensitivity are as follows:

   (1) Sensitive.

   (2) Business-controlled sensitive.

   (3) Nonsensitive.

b. **Criticality of records** measures the need for continuous availability of the records. The three levels in order of decreasing criticality are as follows:

   (1) Critical.

(2) Business-controlled critical.

(3) Noncritical.

c. **Classified records** are records that contain information about the national defense and foreign relations that have been determined under relevant executive orders to require protection against unauthorized disclosure. Classified records in the custody of the Postal Service are managed by the Inspection Service. There are three types of classified records as follows:

(1) Top secret.

(2) Secret.

(3) Confidential.

d. **Vital records** are records that must be available in the event of an emergency in order to ensure the continuity of Postal Service operations and the preservation of the rights and interests of the Postal Service, its employees, suppliers, and customers. Loss of or damage to these records means that the Postal Service would not be able to re-establish normal business operations.

The two types of vital records are as follows:

(1) **Emergency operating records** — Records that are necessary to support essential functions of the Postal Service during and immediately following a national emergency.

(2) **Rights and interests records** — Records that are maintained to ensure the preservation of the rights and interests of the Postal Service, its employees, suppliers, and customers.

If the designation indicated on a record is no longer warranted, the custodian may manage the record in accordance with the business rules for the required designation. Custodians may indicate the new designation on records, as appropriate, by placing a single line through the former designation so that it remains legible.

6-2.4 Micrographics

Micrographics or optical imaging is a technology that reduces any form of information to a microform medium.

6-2.4.1 Microform

Microform is a generic term for any form, either film or paper, that contains micro-images, a unit of information, such as a page of text or drawing, too small to be read without magnification.

6-2.4.2 Policy

Micrographics may be used for the following purposes:

a. Preservation of deteriorating records.

b. Production of archival or intermediate records.

c. Duplication of information for dissemination to other locations.

d. Increased efficiency in searching records.

e. Greater security for sensitive records.

f. Reduction of paper record holdings or use of space.

6-2.4.3 Legal

Federal statute (28 U.S.C. 1732) provides for the legality and admissibility of microforms and electronic images that accurately reproduce or form a durable medium for reproducing the original record. To meet the requirements of this statute, microform records must be produced in the regular course of business and be able to be satisfactorily identified and certified.

Original documents sometimes must be retained to resolve questions of document authenticity. If the authenticity of documents having legal significance could be subject to question, obtain the advice of the Area Managing Counsel's Office (or for Headquarters organizations, the Managing Counsel, Civil Practice) before disposing of the original.

6-2.4.4 Archival

Only original silver halide microfilm has sufficient archival quality to be substituted for documents requiring permanent retention or to produce microforms of permanent retention value.

6-2.4.5 Maintenance and Disposal

Microforms are subject to all regulations on retention, disclosure, privacy, and security of Postal Service records and information.

6-3 Retention

6-3.1 General

The retention periods for records are determined by business, historical, or legal needs of the organization.

6-3.2 Record Series and Record Control Schedules

Postal Service records are grouped into record series. A record series is a group of records that relate to the same subject and have the same retention period. A record control schedule provides for all aspects of records management for a record series including storage, transfer, retention periods, and disposal instructions. All records control schedules will specify a cutoff period. A cutoff period is the termination of a file or information in a file at regular periodic intervals that allows for their disposal or transfer.

6-3.3 Retention Periods

General. Retention periods are contained in the records control schedule for the applicable record series. They are available in eRIMS. Keep records for the period indicated and then dispose of them as specified in section 6-5.

E-Mail Retention. E-mails and their attachments are Postal Service records that must be managed in accordance with Postal Service policies and procedures. Refer to Management Instruction AS-870-2007-7, *Electronic*

Messaging for the retention of e-mails created on, sent from, or received by Postal Service systems.

Extension of Retention Periods. Retention periods may be extended in response to a court order, if subject to a legal hold or needed for a special use. Other records should not be maintained for longer than the periods specified.

6-4 Storage and Retrieval

6-4.1 General

Records should be stored within the control of each department. However, records no longer required for active reference and having a remaining life of more than 1 year, but not yet eligible for destruction, may be transferred to local storage or a Federal Records Center (FRC) unless subject to a legal hold. For information regarding where a record should be stored, see the appropriate records control schedule found in eRIMS.

6-4.2 Local Storage

Local storage may include commercial storage sites or Postal Service facilities. For inactive Headquarters records, personnel should follow storage procedures found in Management Instruction AS-510-97-5, *Storage and Retrieval of Headquarters Records.* Field personnel should check with their facilities manager for transfer and retrieval instructions. All transfers to local Postal Service storage must be accompanied by PS Form 773, *Records Transmittal and Receipt.*

6-4.3 National Archives and Records Administration and Federal Records Centers

The National Archives and Records Administration (NARA) is the government agency that stores and maintains the U.S. Government's permanent collection of documents that records important events in American history. NARA also stores federal government inactive temporary records across the country in secure FRCs.

The following procedures apply with respect to transferring records to the FRCs:

a. **Conditions.** Forward to FRCs only:

   (1) Records series approved by the Records Office and having a remaining life of more than 1 year.

   (2) Volumes of records consisting of 1 cubic foot or more. (The installation must keep quantities of less than 1 cubic foot and destroy them in house when the retention period expires.)

b. **Procedures.** Separated employee personnel and medical records are stored in the National Personnel Records Center (NPRC) in St. Louis, Missouri; for applicable procedures, contact the Records Office. For all other FRCs, use the following procedures:

(1) Assemble records to be shipped and pack (95 percent to capacity) in 1 cubic foot boxes obtained for this purpose from the General Services Administration (Item # 8115-00-117-8249). Prepare a box list, identifying the folders in each box, in duplicate. Insert one copy of the box list in the first box of the accession to be shipped with the records, and retain one copy locally.

(2) Complete two copies of Standard Form (SF)-135, *Records Transmittal and Receipt.* This form may be obtained from the NARA Web site at: *http://www.archives.gov/frc/forms/sf-135-intro.html.* Send both copies to the receiving FRC at least 2 weeks before the intended shipping date.

(3) The FRC shows approval by returning one annotated copy of the SF-135 to the requesting installation.

(4) Place a copy of the SF-135 in the first box of the shipment and ship. Hold a copy in your office until the FRC returns the receipted copy.

(5) File the receipted copies locally in the event they are needed for retrieval of the stored records prior to their disposal.

c. **Location.** See eRIMS or visit the NARA Web site *(http://www.archives.gov/frc/)* for Federal Record Center addresses and areas served.

d. **Retrieval.** The installation from where the records were sent handles their retrieval. For the retrieval process of medical records, contact the Headquarters Medical Program Office. Requests for retrievals are made on Optional Form (OF) 11, *Reference Request — Federal Records Centers,* or through NARA's electronic retrieval system, Centers Information Processing System (CIPS). FEDSTRIP ordering offices order Form OF-11, directly from GSA. Non-FEDSTRIP ordering offices order this form from their supporting supply section or from their GSA Customer Supply Center. Retrievals are made at the Federal Records Centers by the accession number and the box location number recorded on the SF-135 when the records were approved for transfer.

6-4.4 Vital Records

Department heads or their designees, in conjunction with the manager, Records Office, are responsible for reviewing their record series to identify their department's vital records, if any. Vital records should be listed on the *Vital Records Inventory Form,* which can be obtained through the manager, Records Office.

a. Hard-copy Vital Records

(1) The manager, Records Office, designates appropriate hard-copy vital records storage facilities away from the locations housing original hard-copy vital records with safeguards appropriate to ensure the quality and integrity of the vital records.

(2) Unless an alternate process has been set up and approved in writing by the manager, Records Office, when a new hard copy (e.g., paper, microform, or CD) vital record is created or received, the employee responsible for the vital record forwards a copy to his or her Postal Service manager. The record should be clearly labeled as a vital record.

(3) The Postal Service manager or his or her designee contacts the manager, Records Office to review and transfer the copy of the vital record to the appropriate storage facility.

b. Electronic Vital Records

The vice president responsible for the vital record(s) and the chief technology officer verify that an adequate disaster recovery plan is in place for each department's electronic vital records. Information Technology ensures that backup for electronic vital records is located at an appropriate facility away from the locations housing original electronic vital records with safeguards appropriate to ensure the quality and integrity of the vital records.

Postal Service managers should review their departments' *Vital Records Inventory Form* at least once a year to verify that it is current and that each record designated as a vital record continues to warrant that designation. After the Postal Service managers review the *Vital Records Inventory Form,* they should send it to their vice president for approval and transmittal to the manager, Records Office.

6-5 Disposal

6-5.1 General

Postal Service records that are eligible for disposal and not subject to a Legal Hold Notice should be disposed of in accordance with the appropriate records control schedule.

To dispose of records that are maintained at an FRC or commercial storage, a *Records Disposal Notice* (Exhibit 6-5.1) is used. *A Records Disposal Notice* is a written notification that lists records that are eligible for disposal.

Exhibit 6-5.1
Suggested Format for Records Disposal Notice

[Date]

[To]

Records Disposal Notice

[Below or attached] is a list of inactive records for which your office is functionally responsible. The records were transferred to an off-site record storage facility and are now eligible for disposal as indicated. These records will be destroyed 30 days from the date of this Notice, unless we are otherwise notified.

Please provide copies of the list to the managers currently responsible for these records. Each manager should review the list, initial their concurrence with the disposal of their records and return the list to _____. However, if any of these records are to be retained, a contact name and number must be identified. We will then coordinate proposed extensions of the disposal dates.

Records ready for disposal:

Transfer ID Number	Box #	Disposal Date	Reviewed by
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Comments: _____

Please return this completed Notice to: [contact name, number, and address]

6-5.2 Disposal Methods

For disposal methods, do the following:

a. Records authorized for disposition may be disposed of using the following methods:
   (1) Transferring to the National Archives.
   (2) Donating to the Smithsonian Institution, local museums, or historical societies.
   (3) Selling as waste material.
   (4) Discarding.
   (5) Physically destroying.

For guidance on the appropriate disposal method, see eRIMS or contact the Records Office.

b. Hard-copy records with retention periods that have expired and that are not subject to a Legal Hold Notice may be sold as waste paper unless they contain information that cannot be disclosed to the general public, such as personal information. Hard-copy records containing personal information must be destroyed pursuant the applicable Privacy Act systems of records (see Appendix). Any contract for sale

must prohibit the resale of the hard-copy records as records or documents. Film or plastic records may be sold under the same conditions and in the same manner. Hard-copy records that cannot be sold should be destroyed by shredding, pulping or burning.

6-5.3 Disposal Procedures

Follow these disposal procedures:

a. **Records Stored Locally or On-Site.** The records custodian or his or her designee will notify each Postal Service manager of his or her responsibility to dispose of records under his or her jurisdiction via a *Records Disposal Notice.* Specific disposal certification instructions are found on the notice.

b. **Records Stored in Federal Record Centers.** The storing FRC will notify the records custodian 90 days before the scheduled disposal date of records eligible for disposal. The records custodian or designee will provide a *Records Disposal Notice* to the responsible Postal Service manager to certify and return to the records custodian. The *Records Disposal Notice* must be returned within 30 days of receipt.

c. **Electronic Records.** Information technology (IT) is responsible for disposing of electronic records (including e-mails) that are stored in Postal Service systems repositories in accordance with Postal Service records controls schedules. The records custodian or Postal Service manager is responsible for forwarding all relevant Records Disposal Notices to IT for action.

6-6 Separation Procedure (Employee or Non-Employee Available)

6-6.1 General

Separation procedures set forth the process for managing records in the possession, custody, or control of employees who are separating from the Postal Service and suppliers who cease to perform services for the Postal Service.

6-6.2 Separation Procedures

The separation procedures are the following:

a. When a Postal Service manager is aware that an employee will be separating or that a supplier for whose services he or she is responsible will be discontinuing services, the manager must ensure that the employee or supplier completes the appropriate checklist. For HQ, use PS Form 292, *Headquarters Clearance Checklist.* For the field, use PS Form 337, *Clearance Record for Separated Employee.*

b. The employee or the supplier completes the activities specified on the checklist and signs the form to certify that he or she has relinquished

all records (regardless of medium) in his or her possession and submits the form to his or her Postal Service manager.

c. The Postal Service manager reviews the checklist to determine that no exceptions are indicated on the form, takes steps to determine that the activities specified on the form have been performed, and then signs the form. By signing the form, the Postal Service manager certifies that he or she has taken custody of all records (regardless of medium) and authorizes termination of the individual's IT account. IT should immediately terminate the individual's IT account, dispose of records residing in the individual's electronic repositories (unless otherwise designated by the manager), and sign the form to certify that this has occurred. Corporate Personnel Management retains the completed form.

d. The manager is responsible for ensuring that hard-copy and electronic records that should be maintained are transferred to appropriate personnel and that all other records are disposed of per the appropriate record schedule.

6-7 Records Subject to Litigation and Legal Holds

6-7.1 General

For records sought pursuant to subpoena, court order, summons, or regarding matters that are in litigation or likely to become the subject of litigation, the custodian must immediately advise appropriate legal counsel. Records may only be released outside the Postal Service on advice of counsel. Postal Service regulations concerning providing records subject to legal proceedings are contained in 39 CFR 265.11–13.

Legal holds are required to preserve Postal Service records for the purposes of pending or anticipated litigation. The Office of General Counsel is responsible for issuing Legal Hold Notices to ensure that relevant Postal Service records are preserved and for issuing Release Notices when the legal hold is lifted.

6-7.2 Procedures to Follow to Issue a Legal Hold Notice

The procedures to issue a legal hold notice are the following:

a. In connection with any pending or anticipated legal proceeding, investigation, or audit, the Office of General Counsel determines whether it is necessary to issue one or more Legal Hold Notices. In those instances, the Office of General Counsel will develop and issue a Legal Hold Notice.

b. When a legal hold is no longer necessary, the Office of General Counsel will issue a Release Notice.

6-7.3 Procedures to Follow When a Legal Hold Notice Is Issued

The procedures to follow when a Legal Hold Notice is issued are the following:

a. Once a Legal Hold Notice has been issued, records subject to the Notice must be preserved until a Release Notice is issued. Retention schedules for these materials are superseded. Records that are subject to a Legal Hold Notice or that are reasonably likely to be relevant to any pending or anticipated legal proceeding, investigation, or audit must not, under any circumstances, be altered, mutilated, concealed, deleted, destroyed, or otherwise disposed of without the specific authorization of counsel.

b. Recipients of Legal Hold Notices must confirm receipt of the Notice and compliance, as requested by counsel. Recipients should also notify counsel if additional distribution is necessary to other employees or parties.

c. Any employee or party who maintains or controls records subject to the Legal Hold Notice shall manage those items to ensure that they are retained in their original form. Any duplicate of a record that has been altered or annotated in any way is a distinct record and must be retained. If records or items covered by the legal hold are subsequently received, they must also be retained.

d. Failure to preserve a record subject to a Legal Hold Notice can subject the Postal Service and employees to fines, sanctions, and other legal penalties.

This page intentionally left blank

Addendum: Guide for Requesters

The United States Postal Service ("Postal Service") has created this guide for the convenience of individuals ("requesters") requesting records or information from the Postal Service under the Privacy Act of 1974, 5 U.S.C. 552a; Postal Service's privacy regulations, 39 CFR 266; the Freedom of Information Act (FOIA), 5 U.S.C. 552; and the Postal Service's FOIA regulations, 39 CFR 265. To the extent that any information in this guide is not consistent with a federal law or regulation, including regulations of the Postal Service, that law or regulation supersedes the information in this guide.

Part I. Privacy Act Requests

A. Introduction

Individuals ("Requesters") may request notification of or access to records about themselves, request amendment of those records, and request an accounting of disclosures of those records by following the procedures in Part I of this Addendum. Additional information about these procedures can be found in the Postal Service's privacy regulations, 39 CFR 266, which must be read together with the Privacy Act of 1974, 5 U.S.C. 552a. The procedures in Part I of this Addendum apply to all records in systems of records maintained by the Postal Service that are retrieved by an individual's name or personal identifier. To determine whether a particular record is maintained in a system of records, a requester may review the Appendix of this Handbook or the Postal Service's systems of records notices published in the *Federal Register*. The Postal Service processes all Privacy Act requests for access to records under the FOIA, 5 U.S.C. 552, following the rules contained in 39 CFR 265, as necessary, which provides the requester with the greatest access to his or her personal records. For purposes of Part I, records custodians ("custodians") are responsible within their respective units for affording individuals their rights to inspect and obtain copies of records concerning them.

B. Submission of Requests

Requesters must submit inquiries regarding the contents of records systems or access/amendment to personal information in writing in accordance with the procedures described in the applicable system of records notice published in the *Federal Register*, within the Appendix of this Handbook, or to the Privacy and Records Management Office at the following address:

PRIVACY AND RECORDS MANAGEMENT OFFICE
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1101

Submit U.S. Postal Inspection Service requests to:

CHIEF POSTAL INSPECTOR
U.S. POSTAL INSPECTION SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260

Submit Office of Inspector General requests to:

FREEDOM OF INFORMATION ACT/PRIVACY OFFICER
U.S. POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL
1735 NORTH LYNN STREET
ARLINGTON, VA 22209-2020

Inquiries must be clearly marked "Privacy Act Request." 39 CFR 266.5.

C. Content of Requests

Requesters must include the information contained under "Notification Procedure" in the applicable system of records as published in the *Federal Register* or within the Appendix of this Handbook in any inquiry concerning a record maintained in a system of records. Requesters contesting the relevance, accuracy, timeliness, or completeness of a record must submit a statement describing the amendment requested in sufficient detail. In addition, a requester must provide identification sufficient to satisfy the custodian as to the requester's identity prior to accessing a record by complying with one of the following identification verification methods:

- Provision of a completed *Certification of Identity* if the records pertain to the requester: *http://about.usps.com/who-we-are/foia/welcome.htm*;
- Provision of a completed *Privacy Waiver* if the records pertain to another individual: *http://about.usps.com/who-we-are/foia/welcome.htm*; or
- Provision of official photo identification, examples of which are a valid driver's license, unexpired passport, and unexpired federal government-issued employee identification card. 39 CFR 266.5.

D. Responses to Requests

(1) Acknowledgment of Request

A requester will receive acknowledgment of receipt of the request within 10 days. 39 CFR 266.5.

(2) Compliance with Request for Access

Once a record has been located and determined to be releasable, the requester will receive a copy of the record or notification of when and where the record will be available for inspection and copying. 39 CFR 266.5.

(3) Denial of Request for Access

If a record does not exist, does not contain personal information about the requester, or is exempt from disclosure, the requester will receive a reply in writing signed by the custodian or appropriate official denying the request. This reply will include a statement determining the factors of denial, and the right to appeal the denial to the General Counsel. 39 CFR 266.5.

(4) Compliance with Notification Requests

A requester will receive notification if a record has been located in response to a request for notification as to whether a specific system of records contains a record pertaining to the requester. 39 CFR 266.5.

(5) Compliance with Requests for Amendments

If an amendment to a record is determined to be proper, a requester will receive notification when the amendment action is complete. If an amendment to a record is determined to be improper, the requester will receive notification of the determination not to amend, the reason for the refusal, and of the requester's right to appeal, or to submit, in lieu of an appeal, a statement of reasonable length setting forth a position regarding the disputed information to be attached to the contested personal record. 39 CFR 266.5.

E. Requester's Responsibilities When Inspecting Records on Postal Service Property

The requester must provide identification sufficient to satisfy the custodian as to the requester's identity before accessing a record by complying with the following identification verification methods:

- Provision of a completed *Privacy Waiver* if the records pertain to another individual: *http://about.usps.com/who-we-are/foia/welcome.htm*; and
- Provision of official photo identification, examples of which are a valid driver's license, unexpired passport, and unexpired federal government-issued employee identification card.

The requester must agree not to leave Postal Service premises with official records unless specifically given a copy for that purpose by the custodian or the custodian's representative. At the conclusion of the inspection, the requester must sign a statement indicating the requester has reviewed specific records or categories of records. The requester may be accompanied by a person of the requester's choice to aid in the inspection of information and, if applicable, the manual recording or copying of the records if the requester submits a signed statement authorizing the person to do so and discussion of the records occurs in the accompanying person's presence. 39 CFR 266.5.

F. Availability of Assistance

The Privacy and Records Management Office is available to provide a requester with assistance in exercising rights under the Privacy Act and the Postal Service's privacy regulations.

PRIVACY AND RECORDS MANAGEMENT OFFICE
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1101
202-268-2608

39 CFR 266.5.

G. Appeal Procedure

(1) Submission of Appeals

If a request for notification of or to inspect, copy, or amend a record is denied, in whole or in part, or if no determination is made, the requester may appeal to:

GENERAL COUNSEL
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1101

39 CFR 266.6.

(2) Content of Appeals

The requester must submit an appeal in writing within 90 days of the date of denial, or within 90 days of such request, if the appeal is from a failure of the custodian to make a determination. The letter of appeal must include, as applicable:

(a) Reasonable identification of the record to which the requester sought notification, access, or amendment.

(b) A statement of the Postal Service action or failure to act, and of the relief sought.

(c) A copy of the request, of the notification of denial, and of any other related correspondence, if any. 39 CFR 266.6.

(3) Responses to Appeals

The requester will receive an appeal decision in writing and, in the event of a denial, the appeal decision will include the reasons for the denial and district court appeal rights. Any record found on appeal to be incomplete, inaccurate, not relevant, or not timely, will be amended within 30 working days of the date of such findings. 39 CFR 266.6.

(4) Requester's Submission of Statement of Disagreement

If the final decision concerning a request for the amendment of a record does not satisfy the requester, any statement of reasonable length provided by the requester setting forth a position regarding the disputed information will be accepted and attached to the relevant personal record. 39 CFR 266.6.

H. Schedule of Fees

(1) Duplication

For duplicating any paper, micrographic record, publication, or computer report, the fee is $0.15 per page, except that the first 100 pages furnished in response to a particular request must be furnished without charge. The Postal Service may, at its discretion, make user-paid copy machines available at any location. In that event, requesters will be given the opportunity to make copies at their own expense. The Postal Service normally will not furnish more than one copy of any record. If duplicate copies are furnished at the request of the requester; a fee of $0.15 per page is charged for each copy of each duplicate page. 39 CFR 266.7.

(2) Limitations on Fees

No fee will be charged to a requester for the process of retrieving, reviewing, or amending a record pertaining to the requester. 39 CFR 266.7.

Part II. FOIA Requests

A. Introduction

The Freedom of Information Act (FOIA) requires the Postal Service to make Postal Service records available to the public, subject to certain exemptions, exclusions, and other laws allowing the Postal Service to withhold certain types of records and information. It is the policy of the Postal Service to make its official records available to the public to the maximum extent consistent with the public interest. Individuals ("Requesters") may request Postal Service records by following the procedures in Part II of this Addendum. Additional information about these procedures can be found in the Postal Service's FOIA regulations, 39 CFR 265, which should be read together with the FOIA, 5 U.S.C. 552. For purposes of Part II, component means any department or facility within the Postal Service that maintains records.

(1) FOIA Reading Room

The records available to the general public in the Postal Service's public and electronic reading rooms in compliance with the FOIA or within the discretion of the Postal Service include, but are not limited to, the following:

Public Reading Room. The following records are available for inspection and copying by the general public in the public reading room of the Postal Service Headquarters library:

(a) All final opinions and orders made in the adjudication of cases by the judicial officer and administrative law judges.

(b) All final determinations, pursuant to 39 U.S.C. 404(b), to close or consolidate a Post Office or to disapprove a proposed closing or consolidation.

(c) All advisory opinions about the private express statutes issued under 39 CFR 310.6.

(d) All supplier disagreement decisions.

(e) Postal Service manuals, instructions, and other publications that affect the general public that are not listed for sale to the general public.

(f) Records that were or were likely to be routinely processed and disclosed under the FOIA after March 31, 1997.

Electronic Reading Room. Records available in the public reading room described above that were created on or after November 1, 1996, are also maintained in the electronic reading room. In addition, indexes of certain records are maintained in the public and electronic reading rooms, and otherwise made available to the general public to the extent required by the FOIA or within the discretion of the Postal Service.

The Postal Service's electronic reading room may be accessed at *http://about.usps.com/who-we-are/foia/readroom/welcome.htm*.

Postal Service manuals, instructions, and other publications that affect the general public that are available to the general public in the public and electronic reading rooms are also available for inspection by the general public in many Post Offices and other Postal Service facilities. Postal Service publications that are not available to the general public in the public and electronic reading rooms of Postal Service facilities or listed for sale to the general public may be requested by the general public pursuant to the FOIA disclosure provisions (see 4-4).

Note: Records available to the general public may contain redactions to the extent permitted by the FOIA.

(2) Resources

(a) Access the Postal Service's FOIA website at *http://about.usps.com/who-we-are/foia/welcome.htm*.

(b) Access the Postal Service's FOIA Annual Reports at *http://about.usps.com/who-we-are/foia/annual-foia-reports/welcome.htm*.

(c) Access the Postal Service's FOIA regulations at *https://www.gpo.gov/fdsys/pkg/CFR-2017-title39-vol1/pdf/CFR-2017-title39-vol1-part265.pdf*.

(3) Categories of Records

Requesters are encouraged to search *usps.com* and other Postal Service public websites before submitting a FOIA request to the Postal Service because the Postal Service publicly posts a vast array of Postal Service data and information. Some of the categories of Postal Service records can be found in the Appendix of this Handbook. Direct questions about whether the Postal Service has a certain type of record to:

PRIVACY AND RECORDS MANAGEMENT OFFICE
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260

202-268-2608

B. Submission of Requests

A requester must submit a FOIA request to the appropriate FOIA Requester Service Center (RSC). Descriptions of, and contact information for, the various FOIA RSCs can be found at: *http://about.usps.com/who-we-are/foia/service-centers.htm*. For assistance in determining the appropriate FOIA RSC, requesters may contact the USPS HQ FOIA RSC at:

PRIVACY AND RECORDS MANAGEMENT OFFICE
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260

202-268-2608

Also, send requests for listings of Postal Service employee names to the USPS HQ FOIA RSC. 39 CFR 265.3.

C. Form of Requests

A requester must submit a FOIA request to inspect or to obtain a copy of an identifiable Postal Service record in writing and bear the caption "Freedom of Information Act Request" or otherwise be clearly and prominently identified as a request for records pursuant to the FOIA, both on the letter and on the envelope or other cover. Requests for records that are labeled incorrectly may be delayed in reaching the appropriate FOIA RSC. A requester must provide his or her full name and mailing address. A requester may also provide a daytime telephone number or email address to facilitate communication regarding his or her request. 39 CFR 265.3.

D. Content of Requests

Requesters must describe the records sought in sufficient detail to enable Postal Service personnel to locate them with a reasonable amount of effort. Whenever possible, requesters must include specific information about each record sought, such as the type of record (e.g., contract, report, or memorandum); the title or case number of a specific document or report; the topic or subject matter; the name of the office, facility, functional unit, or employees most likely to possess the record; the geographical location, such as a city and state, where the records are thought to exist; the date or general timeframe of the record's creation; and any details related to the purpose of the record. Requests for email records must specify the likely senders and recipients, key words, and a range of dates. If seeking information about a company, requesters must provide the exact name and address of the company (many companies use similar names). Before submitting requests, requesters may contact the relevant Postal Service FOIA RSC to discuss the records they are seeking and to receive assistance in describing the records. The request may state the maximum amount of fees for which the requester is willing to accept liability without prior notice. If no amount is stated, the requester will be deemed willing to accept liability for fees not to exceed $25.00. The request may also specify the preferred form or format (including electronic formats) of the requested records. 39 CFR 265.3.

E. First-Party Requests

Before release of a record, a requester who is making a request for records about himself or herself must provide verification of identity sufficient to satisfy the component as to his or her identity or by completing the *Certification of Identity* available at *http://about.usps.com/who-we-are/foia/welcome.htm*. 39 CFR 265.3.

F. Third-Party Requests

Where a FOIA request seeks disclosure of records that pertain to a third party, a requester may receive greater access by submitting a written authorization signed by that individual authorizing disclosure of the records to the requester, by submitting proof that the individual is deceased (e.g., a copy of a death certificate or an obituary), or by completing the *Privacy Waiver* available at *http://about.usps.com/who-we-are/foia/welcome.htm*. 39 CFR 265.3.

G. Improper Requests

A request that does not reasonably describe the records sought, or does not comply with the published rules regarding the procedures to be followed for submitting a request, will be deemed an improper FOIA request. If after receiving a request, the Postal Service determines that it is improper, the Postal Service will inform the requester as to why the request is improper. If the requester fails to respond to the Postal Service's request for clarification or additional information within 30 calendar days, the Postal Service will assume the requester is no longer interested in pursuing the request and close its file. The FOIA RSCs and the FOIA Public Liaisons are available to assist requesters in correcting a request that does not reasonably describe the records sought. 39 CFR 265.3.

H. Timing of Responses to Requests

Requests will ordinarily be responded to according to their order of receipt. A request that is not initially submitted to the appropriate FOIA RSC will be deemed to have been received by the Postal Service at the time that it is actually received by the appropriate FOIA RSC; but in any case, a request will be deemed to have been received no later than 10 business days after the request is first received by a FOIA RSC. 39 CFR 265.5.

(1) Acknowledgment of Requests

A request will be acknowledged in writing with an individualized tracking number and brief description of the records sought if it will take longer than 10 working days to process. 39 CFR 265.4.

(2) Statutory Time Limit

Under the FOIA, the Postal Service is required to respond to a FOIA request within 20 working days of receipt of the request, unless unusual circumstances or exceptional circumstances are applicable. 5 U.S.C. 552. The complexity of the request, number of records potentially responsive to the request, number of facilities with responsive records, and the need to consult with other agencies are factors that could cause delays in processing the request. Requesters are encouraged to narrow the scope of a FOIA request with the assistance of the Privacy and Records Management Office.

(3) Aggregation of Requests

If a requester submits multiple requests or acts in concert with others to submit multiple requests and such requests are determined to constitute a single request, the requests will be aggregated. 39 CFR 265.5.

(4) Multitrack Processing

Unless expedited processing has been granted, the Postal Service places each request in simple or complex tracks based on the amount of work and time involved in processing the request. Within each track, the Postal Service processes requests in the order in which they are received. When appropriate, the FOIA RSC or the component will notify the requester if it has placed the request in the “Complex” track, and provide the requester with an opportunity to limit the scope of the request. If the requester limits the scope of the request, it may result in faster processing. 39 CFR 265.5.

(5) Expedited Processing

Requests and appeals will be processed on an expedited basis whenever it is determined that they involve:

(a) Circumstances in which the lack of expedited processing could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(b) An urgency to inform the public about an actual or alleged Federal Government activity, if made by a person who is primarily engaged in disseminating information.

A requester who seeks expedited processing must submit a statement, certified to be true and correct, explaining in detail the basis for making the request for expedited processing. A requester will receive notification within 10 calendar days of the receipt of a request for expedited processing of the decision whether to grant or deny expedited processing. If expedited processing is granted, the request will be given priority, placed in the processing track for expedited requests, and processed as soon as practicable. If a request for expedited processing is denied, any appeal of that decision will be acted on expeditiously. 39 CFR 265.5.

(6) Unusual Circumstances

If unusual circumstances, as defined in the FOIA, apply to a request, the requester will receive notification of the unusual circumstances before the expiration of the 20-day statutory time limit with an extension of 10 working days. Where the extension exceeds 10 working days, the requester will receive notification that offers the opportunity to modify the request and arrange an alternative processing time period, and provides information about the availability of the Office of Government Information Services dispute resolution services. 39 CFR 265.5.

I. Responses to Requests

(1) Grants of Requests

A requester will receive a written determination granting a request in whole or in part and stating if any fees were charged. Upon payment of any applicable fees, the requester will promptly receive the requested records. 39 CFR 265.6.

(2) Adverse Determinations of Requests

A requester will receive an adverse determination denying a request in writing. Adverse determinations or denials of requests include decisions that:

(a) The requested record is exempt, in whole or in part;

(b) The request does not reasonably describe the records sought;

(c) The information requested is not a record subject to the FOIA;

(d) The requested record does not exist, cannot be located, or has been destroyed; or

(e) The requested record is not readily reproducible in the form or format sought by the requester.

Adverse determinations also include denials involving fees or fee waiver matters, or denials of requests for expedited processing. 39 CFR 265.6

J. Administrative Appeals

(1) Requirements for Making an Appeal

Requesters may appeal adverse decisions rendered by the Postal Inspection Service or any Postal Service component by mail to:

GENERAL COUNSEL
U.S. POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260

foiaappeal@usps.gov

The requester must make the appeal in writing. To be considered timely, it must be postmarked, or in the case of electronic submissions, transmitted within 90 calendar days after the date of the response or within a reasonable time if the appeal is from a failure of the component to act. A letter of appeal must include, as applicable:

(a) A copy of the request, of any notification of denial or other action, and of any other related correspondence;

(b) The FOIA tracking number assigned to the request;

(c) A statement of the action, or failure to act, from which the appeal is taken;

(d) A statement identifying the specific redactions to responsive records that the requester is challenging;

(e) A statement of the relief sought; and

(f) A statement of the reasons why the requester believes the action or failure to act is erroneous. 39 CFR 265.8.

(2) Adjudication of Appeals

The General Counsel will give prompt consideration to an appeal for expedited processing of a request. All other decisions normally will be made within 20 working days from the time of the receipt by the General Counsel. 39 CFR 265.8.

(3) Appeal Decisions

A requester will receive an appeal decision in writing. An appeal decision that upholds a component's determination in whole or in part will contain a statement that explains the reasons for the affirmance, the FOIA exemptions applied, the requester's statutory right to file a lawsuit, and the mediation services offered by the Office of Government Information Services of the National Archives and Records Administration as a non-exhaustive alternative to litigation. If a custodian's decision is remanded for further processing, the requester will be notified of that determination in writing and instructed to await a response directly from the component. 39 CFR 265.8.

(4) When Appeal is Required

Before seeking judicial review of a component's adverse determination, a requester generally must first submit a timely administrative appeal. 39 CFR 265.8.

K. Fees

The Postal Service charges search, review, and duplication fees based on the category of the requester. For more information on types of fees and requester categories, see the definitions found in 39 CFR 265.9(b). The Postal Service ordinarily will collect all applicable fees from the requester before sending copies of records to the requester. Requesters must pay fees by check or money order made payable to the "U.S. Postal Service." 39 CFR 265.9.

(1) Requester Categories

A requester is placed in a requester category for the purposes of assessing fees based on the requester's intended use of the records as stated in the requester's FOIA request. For more information on requester categories, see the definitions found in 39 CFR 265.9(b).

(a) A commercial-use requester is a requester who asks for information for a use or purpose that furthers the commercial, trade, or profit interest, which can include furthering those interests through litigation.

(b) An educational institution is any school that operates a program of scholarly research.

(c) A noncommercial scientific institution is an institution that is not operated on a "commercial" basis, but operated solely for the purpose of conducting scientific research the results of which are not intended to promote any particular product or industry.

(d) A representative of the news media is any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.

(2) Search Fees

Search is the process of looking for and retrieving records or information responsive to a request. Search time includes page-by-page or line-by-line identification of information within records and the reasonable efforts expended to locate and retrieve information from electronic records. Except for requests made by educational institutions, noncommercial scientific institutions, or representatives of the news media, all other requesters are subject to search fees. The Postal Service may charge for time spent searching even if no responsive records are located or if it determines that the records are entirely exempt from disclosure.

(a) The search fee is $21.00 for each half hour spent by personnel searching for requested records, including electronic searches that do not require new programming.

(b) Requesters will be charged the direct costs associated with conducting any search that requires the creation of a new computer program to locate the requested records. Requesters will be notified of the costs associated with creating such a program and must agree to pay the associated costs before the costs may be incurred.

(c) For requests that require the retrieval of records stored at a federal records center operated by the National Archives and Records Administration (NARA), or other storage facility, additional costs may be charged for their retrieval. 39 CFR 265.9.

(3) Duplication Fees

Duplication is reproducing a copy of a record or of the information contained in it and is necessary to respond to a FOIA request. All requesters are subject to duplication fees. The duplication fee is $0.15 per page for records in hard copy format. The duplication fee for producing records on tapes, disks, or other media is the direct cost of producing the copy, including operator time. Where paper documents must be scanned in order to comply with a requester's preference to

receive the records in an electronic format, the requester will be charged the direct costs associated with scanning those materials. For other forms of duplication, the requester will be charged the direct costs. 39 CFR 265.9.

(4) Review Fees

Review is the examination of a record located in response to a request in order to determine whether any portion of it is exempt from disclosure. Review time includes processing any record for disclosure, such as doing all that is necessary to prepare the record for disclosure, including the process of redacting the record and marking the appropriate exemptions. Commercial-use requesters will be charged review fees at the rate of $21.00 for each half hour spent by personnel reviewing the requested records.

(5) Restrictions on Charging Fees

(a) Educational institutions (unless the records are sought for a commercial use), noncommercial scientific institutions, and representatives of the news media are not required to pay search fees.

(b) Except in certain instances described in 39 CFR 265.9(d)(2), requesters will not be charged search fees if the component fails to respond within the statutory time limits.

(c) No search or review fees will be charged for a quarter-hour period unless more than half of that period is required for search or review.

(d) With the exception of commercial-use requesters, all other requesters are entitled to the first two hours of search time and the first 100 pages of duplication free of charge. No fee will be charged if the remaining balance is $25.00 or less after the first 100 free pages and two hours of search time are deducted from the balance. 39 CFR 265.9.

(6) Aggregating requests.

In instances where the Postal Service reasonably believes that a requester or a group of requesters acting in concert is attempting to divide a single request into a series of requests for the purpose of avoiding fees, or that a requester or group of requesters acting in concert makes multiple requests for the same records maintained at multiple facilities or components, the Postal Service may aggregate those requests and charge accordingly. Multiple FOIA requests by a single requester related to the same issue will be aggregated for the purpose of assessing fees. 39 CFR 265.9.

(7) Advance payments.

A requester will be required to make an advance payment up to the amount of the entire anticipated fee if the total fee is estimated to exceed $250.00. Where a requester has previously failed to pay a properly charged FOIA fee within 30 calendar days of the billing date, the requester will be required to pay the full amount due on that prior request, and make an advance payment of the full amount of any anticipated fee before the Postal Service will process a new request or continues to process a pending request or any pending appeal. In cases when advance payment is required, the FOIA request will not be considered received and further work will not be completed until the required payment is received. If the requester does not pay the advance payment within 30 calendar days of the date of the fee determination letter, the request will be administratively closed. 39 CFR 265.9.

(8) Requirements for Waiver or Reduction of Fees

A requester must request a waiver or reduction of fees when first submitting a FOIA request to the Postal Service. A requester is entitled to a waiver or reduction of fees if the requester demonstrates the following:

(a) Disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Postal Service, and

(b) Disclosure of the information is not primarily in the commercial interest of the requester.

Additional guidance on these requirements can be found at 39 CFR 265.9(j).

Appendix

Privacy Act Systems of Records

Section A. Explanation

This appendix includes Section A. - relating to systems of records under the Privacy Act.

Section B. contains an overview of the Privacy Act and its protections.

Section C. is a complete index of Postal Service systems of records.

Section D. describes disclosures authorized by statute and the standard routine uses that apply to all systems of records.

Section E. contains the complete text of Postal Service systems of records.

Section B. Privacy Act Protections

The Privacy Act of 1974, 5 U.S.C. 552a, applies to Federal agencies, including the Postal Service. The Privacy Act provides protections for personal information that an agency maintains in a system of records. A system of records describes a file, database, or program from which information is retrieved about an individual by name or other personal identifier.

The Privacy Act establishes recordkeeping, access, and nondisclosure requirements for information maintained in a system of records. The Privacy Act requires agencies to publish a description of each system of records to provide full information on how personal information within the system of records is treated. This description includes how information is collected, used, disclosed, stored, and disposed of. It also includes how individuals can obtain access to, correct, and amend information about them that is included in the system of records.

The Privacy Act places limitations and requirements on how information from within a system of records can be disclosed, as described in Section D.

Section C. Index of Systems of Records

Part I. General Systems

Part II. Customer Systems

Section D. Authorized Disclosures and Routine Uses

Under the Privacy Act, information can only be disclosed from a system of records, internally or externally, under one of two conditions:

1. The individual has authorized the disclosure in writing.
2. The disclosure fits within one of twelve specified categories.

The following is a description of disclosures, including those authorized by the Privacy Act and USPS regulations and routine uses.

D.1. Disclosures Authorized by the Privacy Act

The Privacy Act authorizes disclosures in the following twelve circumstances:

1. To agency employees who need the information to perform their job.
2. As required by the Freedom of Information Act.
3. For routine uses for which the agency has provided proper notice.
4. To the Bureau of the Census for purposes related to census and survey activities.
5. To a recipient who provides advance written assurance that the information will only be used for statistical research or reporting, and the information provided does not identify individuals.
6. To the National Archives and Records Administration for historic preservation purposes.
7. To other domestic government agencies for a civil or criminal law enforcement activity if the activity is authorized by law. In such cases, the agency head must specify in writing both the law enforcement activity and the particular information needed.
8. To a person upon a showing of compelling circumstances affecting an individual's health or safety. The agency must send notice of the disclosure to the individual's last known address.
9. To Congress, or to the extent the matter is within their jurisdiction, to any of its committees or subcommittees.
10. To the Comptroller General in the performance of duties of the Government Accountability Office.
11. Pursuant to the order of a court of competent jurisdiction.
12. To a consumer reporting agency in order to collect claims owed to the Government.

The Privacy Act allows agencies to disclose information from a system of records if they establish a routine use describing the disclosure (see #3. above). Under the Privacy Act, routine uses are defined as disclosures that are compatible with the purpose for which the information was collected — in other words, disclosures that are appropriate and necessary for the efficient conduct of government business. Routine uses for each system of records are established by publishing them in a *Federal Register* notice that describes the system. They must also be disclosed in a notice given to an individual when information is collected directly from the individual. The Privacy Act also allows disclosures required by the Freedom of Information Act (FOIA) (see #2 above). USPS regulations implementing the Privacy Act and FOIA are contained in 39 CFR Parts 261-268.

D.2. Standard Routine Uses

The following standard routine uses apply to USPS systems of records. In general, standard routine uses 1. through 9. apply to general systems — systems relating to employees, finance, investigations, litigation, and other systems not primarily related to USPS customers. General systems are listed in Section C, Part I. In general, standard routine uses 1. through 7., 10., and 11. apply to customer systems. These systems, which contain information related to USPS customers, are listed in Section C, Part II. The specific standard routine uses applicable to each system of records, as well as any special routine uses, are described in each system of records in E.

1. *Disclosure Incident to Legal Proceedings*. When the Postal Service is a party to or has an interest in litigation or other legal proceedings before a federal, state, local, or foreign adjudicative or administrative body or before an arbitrator, arguably relevant records may be disclosed before that body, and/or to the Department of Justice or other legal counsel representing the Postal Service or its employees, and to actual or potential parties or their representatives in connection with settlement discussions or discovery. Arguably relevant records may also be disclosed to former Postal Service employees or suppliers when reasonably necessary to elicit information related to actual or potential litigation. Arguably relevant records may be disclosed to a bar association or similar federal, state, or local licensing or regulatory authority that relate to possible disciplinary action.
2. *Disclosure for Law Enforcement Purposes*. For information derived from general systems, when the Postal Service becomes aware of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, or in response to the appropriate agency's request on a reasonable belief that a violation has occurred, records may be referred to the appropriate agency, whether federal, state, local, or foreign, charged with enforcing or implementing the statute, rule, regulation, or relevant order. For records derived from customer systems, records may be disclosed to appropriate law enforcement agencies to investigate, prevent, or take action regarding suspected illegal activities against the Postal Service; and such customer records may only otherwise be disclosed to law enforcement agencies as required by law.
3. *Disclosure to Congressional Office.* Records about an individual may be disclosed to a congressional office in response to an inquiry from the congressional office made at the prompting of that individual.
4. *Disclosure to Agents or Contractors.* Records may be disclosed to entities or individuals under contract or agreement with the Postal Service when necessary to fulfill a Postal Service function, to provide Postal Service products or services to customers, or to provide the contractor with investigative or performance records about the contractor's employees.
5. *Disclosure to Auditors.* Records may be disclosed to government agencies and other entities authorized to perform audits, including financial and other audits, of the Postal Service and Postal Service activities.

6. *Disclosure to Labor Organizations.* As required by applicable law, records may be furnished to a labor organization when needed by that organization to perform its duties as the collective bargaining representative of Postal Service employees in an appropriate bargaining unit.
7. *Disclosure to Government Agencies*. Records may be disclosed to a federal, state, local, or foreign government agency when necessary in connection with decisions by the requesting agency or by the Postal Service regarding personnel matters, issuance of security clearances, letting of contracts, or decisions to issue licenses, grants, or other benefits. With respect to employee records, such matters include provision of parent locator services; enforcement of child support, tax, and debt obligations; and claims, investigations, and inspections related to occupational safety, injuries, illnesses, and accidents.
8. *Disclosure to Equal Employment Opportunity Commission.* Records may be disclosed to an authorized investigator, administrative judge, or complaints examiner appointed by the Equal Employment Opportunity Commission when requested in connection with the investigation of a formal complaint of discrimination filed against the Postal Service under 29 CFR Part 1614.
9. *Disclosure to Merit Systems Protection Board or Office of the Special Counsel.* Records may be disclosed to the Merit Systems Protection Board or Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies, investigations of alleged or possible prohibited personnel practices, and such other functions as may be authorized by law.
10. *Disclosure to Agencies and Entities for Financial Matters.* Records may be disclosed to credit bureaus, government agencies, and service providers that perform identity verification and credit risk assessment services; to financial institutions or payees to facilitate or resolve issues with payment services; or to government or collection agencies for the purposes of debt collection or responding to challenges to such collection.
11. *Disclosure for Customer Service Purposes.* Records may be disclosed to entities if the disclosure is part of the service to the customer. This includes disclosures to addressees of mail to process inquiries and claims; entities to which the customer wants to provide identity verification; the State Department for passport processing; international posts or agents to facilitate or process international services, claims, or inquiries; and mailers of sexually oriented advertisements to provide a list of customers who do not want to receive them.

D.3. Exempted Systems of Records

Certain categories of records contained in the systems of records below are exempt from the following Privacy Act provisions: to release records; to maintain only relevant and necessary information; to establish notification, access, and contest procedures or publish them in a *Federal Register* notice; and to release an accounting of disclosures.

100.100 Recruiting, Examining, and Placement Records
100.300 Employee Development and Training Records
100.600 Personnel Research Records
200.000 Labor Relations Records
500.300 Emergency Management Records
700.000 Inspection Service Investigative File System
700.100 Mail Cover Program Records
700.300 Inspector General Investigative Records
860.000 Financial Transactions

In addition to the above, certain categories of records contained in the systems of records below are exempt from the following Privacy Act provisions: to collect information directly from the individual; to provide notice to the individual when collecting information; to maintain accuracy, relevance, timeliness, and completeness of records; to provide notice of a correction or notation; to serve notice upon disclosure under compulsory legal process; to apply civil remedies; and to apply provisions to contractors.

500.300 Emergency Management Records
700.000 Inspection Service Investigative File System
700.100 Mail Cover Program Records
700.300 Inspector General Investigative Records

The legal authority and statutory references for all exemptions are contained in 39 CFR 266.9.

Section E. Complete Text of Systems of Records

USPS100.000 System Name: General Personnel Records.

System Location

All USPS facilities and personnel offices; Intergrated Business Solutions Services Centers; National Personnel Records Center; Human Resources Information Systems; Human Resources Shared Services Center; Headquarters; Computer Operations Service Centers; and contractor sites.

Categories of Individuals Covered by the System

Current and former USPS employees, their family members, and former spouses who apply and qualify for federal employee benefits under public law.

Categories of Records in the System

1. Employee, former employee, and family member information: Name(s), Social Security Number(s), Employee Identification Number, date(s) of birth, place(s) of birth, marital status, postal assignment information, work contact information, home address(es) and phone number(s), personal email address, finance number(s), duty location, and pay location.
2. *Official Personnel Folder (OPF) or eOPF (electronic version):* Records related to appointment support, prior federal civilian employment, postal employment, personnel actions, anniversary dates, retirement, benefits, and compensation.
3. *Automated employee information:* Records generated, approved, and stored by electronic means such as *Notification of Personnel Actions,* health benefit elections, tax withholding changes, and address changes.
4. *Reference copies of all discipline or adverse actions:* Letters of warning; notices of removal, suspension and/or reduction in grade or pay; letters of decisions; and documents relating to these actions. These are used only to refute inaccurate statements by witnesses before a judicial or administrative body. They may not be maintained in the employee's OPF or eOPF but must be maintained in a separate file by Labor Relations.
5. *Nonbargaining unit employee discipline, grievance, and appeals records.*
6. *Job bidding records:* Records related to the employee's bid for a preferred assignment.
7. *Biographical summaries:* Records and photographs used for public relations purposes.
8. *Level 2 supervisors' notes:* Records of discussions, letters of warning, and any other relevant official records being maintained at the supervisor's discretion for the purpose of enabling effective management of personnel. (A level 2 supervisor directly supervises bargaining unit employees.)
9. *Email Addresses:* personal email address(es) for retired employees are retained in a separate database and file from other current and former employee information.

Authority for Maintenance of the System

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

Purpose(s)

1. To perform routine personnel functions.
2. To maintain a source of readily available information on employees for administrative purposes.
3. To administer the grievance and appeal procedure for nonbargaining unit employees.
4. To match a vacant position to the most qualified candidate in bids for preferred assignment.
5. To provide public relations information on USPS management personnel.
6. To provide federal benefit information to retired employees.

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. Job bidding records may be disclosed on official bulletin boards in Postal Service facilities and to supervisory and other managerial organizations recognized by USPS.
b. Records pertaining to financial institutions and to nonfederal insurance carriers and benefits providers elected by an employee may be disclosed for the purposes of salary payment or allotments, eligibility determination, claims, and payment of benefits.
c. Records may be disclosed to the National Labor Relations Board (NLRB) in response to its request for investigative purposes, to the extent that the requested information is relevant and necessary.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, digital files, and paper files. Duplicates of records in the OPF or eOPF and automated employee data may be maintained for localized employee administration or supervision. Records may be filed at offices other than where OPF or eOPF is located, or may be duplicated at a site closer to where the employee works.

Retrievability

By name, Social Security Number, Employee Identification Number, or duty or pay location.

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. Nonbargaining unit employee discipline, grievance, and appeals records maintained outside the OPF (hard or soft copy) are kept in locked filing cabinets or secured record storage rooms; and related automated records are protected with password security. 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.

Retention and Disposal

1. Permanent OPF or eOPF records are permanently retained. Temporary OPF or eOPF records are generally retained 2 years and are purged upon the employee's separation from USPS.
2. Except as otherwise provided by a collective bargaining agreement, original or copies of discipline or adverse actions are maintained up to 2 years; or, if an additional or more recent disciplinary action has been taken, for a longer period. After 2 years, or lesser time specified in the decision, the employee may request the disciplinary record be purged from the OPF or eOPF provided no subsequent discipline was issued. Records that support a PS Form 50, *Notification of Personnel Action,* e.g., the separation of an employee for cause or the resignation of an employee pending charges, are considered permanent records and may not be purged at the request of an employee.
3. Reference copies of discipline or adverse actions. These records are kept for historical purposes and are not to be used for decisions about the employee. The retention of these records may not exceed 10 years beyond the employee's separation date. The records are maintained longer if the employee is rehired during the 10-year period. They may not be maintained in the employee's OPF or eOPF, but must be maintained in a separate file by Labor Relations.
4. Grievance and appeal records of nonbargaining unit employees are retained 7 years.
5. Job bidding records are retained 2 years.
6. Biographical summaries are retained for the duration of employment.
7. Records to provide federal benefit information to retired employees are retained for 10 years. Records may be purged at the request of the retired employee.

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.

System Manager(s) and Address

Director of Human Resources, USPS OIG, 1735 N. Lynn Street, 10th floor, Arlington, VA 22209.

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Notification Procedure

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

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; employees' supervisors; USPS customers; law enforcement agencies; individuals who are personal references; former employers, including other federal agencies; and other systems of records.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 100.100 System Name: Recruiting, Examining, and Placement Records.

System Location

Pre-employment investigation records are located at USPS Human Resources (HR) offices and contractor locations, except for drug screening and medical examination records, which are maintained in USPS medical facilities and designee offices.

Recruiting, examining, and placement records are located at USPS HR offices, Headquarters, Human Resources Shared Services Center, Integrated Business Solutions Services Centers, the Bolger Center for Leadership Development, the National Center for Employee Development, and contractor locations.

Categories of Individuals Covered by the System

Current and former USPS employees, applicants for employment, and potential applicants with candidate profiles.

Categories of Records in the System

1. Applicant, potential applicants with candidate profiles, and employee information: Name(s), Social Security Number(s), Candidate Identification Number, Employee Identification Number, date(s) of birth, postal assignment or vacancy/job posting history information, work contact information, home address(es) and phone number(s), personal email address, finance number(s), duty location, and pay location.
2. Pre-employment investigation information: Records compiled by USPS, including criminal, employment, military, and driving records; drug screening and medical assessment results. Also includes Special Agency Check with Inquiries (SACI) and National Agency Check with Inquiry (NACI): Investigative records requested by USPS and compiled by the Office of Personnel Management (OPM) for newly hired employees, including postal inspectors' investigative reports.
3. Recruiting, examining, and placement information: Records related to candidate profiles, applications, test results, interview documentation, and suitability screening.

Authority for Maintenance of the System

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

Purpose(s)

1. To determine suitability for employment.
2. To provide managers, HR personnel, and medical officers with information for recruiting and recommending appointment of qualified individuals.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By applicant or employee name, Social Security Number, Candidate Identification Number, Employee Identification Number, duty or pay location, or posting/vacancy to which application was made.

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.

Retention and Disposal

1. Preemployment investigation records are retained 10 years from the date the individual is initially found suitable for employment, or 10 years from the date action was taken to deny or terminate employment.
2. Candidate information and Candidate Identification Number are retained for a minimum of 2 years. Vacancy files, including applicant/employee name, identification number, posting/vacancy number, and information supplied by applicant/employee in response to the vacancy posting, are retained 5 years. Employment registers are retained 10 years. Certain forms related to a successful applicant are filed in the electronic Official Personnel Folder as permanent records.
3. Paper examining answer sheets are retained 6 months; and computer media copies are retained 10 years. Scanned Maintenance Selection System forms are retained 10 years, and related hiring lists are retained 5 years.

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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system must address inquiries to Human Resources Shared Services Center, P.O. Box 970400, Greensboro, NC 27497-0400. Inquiries must include full name,

Candidate Identification Number (as provided during the application process) or Employee Identification Number, name and address of facility where last employed, and dates of USPS employment or date of application.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Applicants; potential applicants with candidate profiles; OPM; police, driving, and military records; former employers and named references; medical service providers; school officials; other federal agencies; and state divisions of vocational rehabilitation counselors.

Systems Exempted From Certain Provisions of the Act

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.

USPS 100.200 System Name: Employee Performance Records.

System Location

USPS facilities where employee performance is evaluated or measured.

Categories of Individuals Covered by the System

Current and former USPS employees, including supervisors and managers who are responsible for a work location.

Categories of Records in the System

1. *Employee information:* Name, Social Security Number, Employee Identification Number, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Employee performance information:* Records related to individual performance evaluation; reports about supervisors and managers who are responsible for a work location; employee recognition; and safe driver awards.

Authority for Maintenance of the System

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

Purpose(s)

1. To provide managers and supervisors with decision-making information for training needs, promotion, assignment considerations, or other job-related actions.
2. To administer achievement award programs and pay for performance.
3. To improve relations and communication between managers and employees by soliciting employee feedback, and to improve management and supervisor leadership skills.

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. When records about the receipt of an award by an employee, including driver safety records, are of news interest and consistent with the public's right to know, the records may be disclosed to the news media or the National Safety Council.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By employee name, Social Security Number, Employee Identification Number, or duty or pay location.

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.

Retention and Disposal

1. Pay for performance evaluation records are retained 5 years. Individual performance evaluations are retained 5 years or until separation of the employee, whichever comes first.
2. Incentive award records are retained 7 years. Length of service award records are retained 1 year. Non-USPS awards are retained 2 years. Letters of commendation and appreciation (excluding permanent copies filed in the OPF or eOPF) are retained 2 years.
3. Employee survey records are retained 5 years.
4. Safe Driver Award records are retained 2 years from date of separation, expiration of license, rescission of authorization, transfer of driver into a nondriving status, or other transfer, whichever comes first.

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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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. 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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees and employees' supervisor or manager.

USPS 100.300
System Name:
Employee Development and Training Records.

System Location

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

Categories of Individuals Covered by the System

Current and former USPS employees.

Categories of Records in the System

1. *Employee information:* Name, Social Security Number, Employee Identification Number, 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.

Authority for Maintenance of the System

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

Purpose(s)

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.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

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

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.

Retention and Disposal

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.

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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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. 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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

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

Systems Exempted From Certain Provisions of the Act

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.

USPS 100.400 System Name: Personnel Compensation and Payroll Records.

System Location

USPS Area and District Human Resources offices, the Human Resources Shared Services Center, Integrated Business Solutions Services Centers, Computer Operations Services Centers, Accounting Services Centers, other area and district facilities, Headquarters, contractor sites, and all organizational units.

Categories of Individuals Covered by the System

1. Current and former USPS employees and postmaster relief/leave replacement employees.
2. Current and former employees' family members, beneficiaries, and former spouses who apply and qualify for benefits.
3. An agent or survivor of an employee who makes a claim for loss or damage to personal property.

Categories of Records in the System

1. *Employee and family member information:* Name(s), Social Security Number(s), Employee Identification Number, ACE ID, date(s) of birth, postal assignment information, work contact information, home address(es) and phone number(s), finance number(s), occupation code, occupation title, duty location, and pay location.
2. *Compensation and payroll information:* Records related to payroll, annual salary, hourly rate, Rate Schedule Code (RSC) or pay type, payments, deductions, compensation, and benefits; uniform items purchased; proposals and decisions under monetary awards; suggestion programs and contests; injury compensation; monetary claims for personal property loss or damage; and garnishment of wages.

Authority for Maintenance of the System

39 U.S.C. 401, 409, 410, 1001, 1003, 1004, 1005, and 1206; and 29 U.S.C. 2601 et seq.

Purpose(s)

1. To support all necessary compensation and payroll activities and related management functions.
2. To generate lists of employee information for home mailings, dues membership, and other personnel support functions.
3. To generate retirement eligibility information and analysis of employees in various salary ranges.
4. To administer the purchase of uniforms.
5. To administer monetary awards programs and employee contests.
6. To detect improper payment related to injury compensation claims.
7. To adjudicate employee claims for loss or damage to their personal property in connection with or incident to their postal duties.
8. To process garnishment of employee wages.
9. To support statistical research and reporting.
10. To generate W-2 and 1095-C information for use with external third party tax preparation services at the request of the individual employee.

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. Records pertaining to financial institutions and to nonfederal insurance carriers and benefits providers elected by an employee may be disclosed for the purposes of salary payment or allotments, eligibility determination, claims, and payment of benefits.

b. Records pertaining to supervisors and postmasters may be disclosed to supervisory and other managerial organizations recognized by USPS.

c. Records pertaining to recipients of monetary awards may be disclosed to the news media when the information is of news interest and consistent with the public's right to know.

d. Disclosure of records about current or former Postal Service employees may be made to requesting states under an approved computer matching program to determine employee participation in, and eligibility under, unemployment insurance programs administered by the states (and by those states to local governments), to improve program integrity, and to collect debts and overpayments owed to those governments and their components.

e. Disclosure of records about current or former Postal Service employees may be made to requesting federal agencies or nonfederal entities under approved computer matching programs to make a determination of employee participation in, and eligibility under, particular benefit programs administered by those agencies or entities or by USPS; to improve program integrity; to collect debts and overpayments owed under those programs and to provide employees with due process rights prior to initiating any salary offset; and to identify those employees who are absent parents owing child support obligations and to collect debts owed as a result.

f. Disclosure of records about current or former Postal Service employees may be made, upon request, to the Department of Defense (DoD) under approved computer matching programs to identify Postal Service employees who are ready reservists for the purposes of updating DoD's listings of ready reservists and to report reserve status information to USPS and the Congress; and to identify retired military employees who are subject to restrictions under the Dual Compensation Act and to take subsequent actions to reduce military retired pay or collect debts and overpayments.

g. Disclosure of records may be made to the Internal Revenue Service under approved computer matching programs to identify current or former Postal Service employees who owe delinquent federal taxes or returns and to collect the unpaid taxes by levy on the salary of those individuals pursuant to Internal Revenue Code; and to make a determination as to the proper reporting of income tax purposes of an employee's wages, expenses, compensation, reimbursement, and taxes withheld and to take corrective action as warranted.

h. Disclosure of the records about current or recently terminated Postal Service employees may be made to the Department of Transportation (DOT) under an approved computer matching program to identify individuals who appear in DOT's National Driver Register Problem Driver Pointer System. The matching results are used only to determine as a general matter whether commercial license suspension information within the pointer system would be beneficial in making selections of USPS motor vehicle and tractor-trailer operator personnel and will not be used for actual selection decisions.

i. Disclosure of records about current or former Postal Service employees may be made to the Department of Health and Human Services under an approved computer matching program for further release to state child support enforcement agencies when needed to locate noncustodial parents, to establish and/or enforce child support obligations, and to locate parents who may be involved in parental kidnapping or child custody cases.

j. Disclosure of records about current or former Postal Service employees may be made to the Department of the Treasury under Treasury Offset Program computer matching to establish the identity of the employee as an individual owing a delinquent debt to another federal agency and to offset the salary of the employee to repay that debt.

k. Disclosure of employment and wage data records about current Postal Service employees may be made to the Bureau of Labor Statistics for use in their Occupational Employment Statistics program for the purpose of developing estimates of the number of jobs in certain occupations, and estimates of the wages paid to them.

l. Disclosure of W-2 and 1095-C tax information records to external third party tax preparation services.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By employee name, Social Security Number, Employee Identification Number, or duty or pay location.

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.

Retention and Disposal

1. Leave application and unauthorized overtime records are retained 3 years. Time and attendance records (other than payroll) and local payroll records are retained 3 years. Automated payroll records are retained 10 years.
2. Uniform allowance case files are retained 3 years; and automated records are retained 6 years.
3. Records of monetary awards with a status that they have been processed, failed processing, cancelled, or reported (Service Award Pins, Retirement Service Awards, Posthumous Service Awards) are retained 7 years, as payroll records would have been affected/processed. Records of award submissions with the status approved, deleted, or as a draft are retained 31 days, as payroll records would not have been affected/processed.
4. Records of employee-submitted ideas are maintained for 90 days after being closed.
5. Injury compensation records are retained 5 years. Records resulting in affirmative identifications become part of a research case file, which if research determines applicability, become either part of an investigative case record or a remuneration case record that is retained 2 years beyond the determination.
6. Monetary claims records are retained 3 years.
7. Automated records of garnishment cases are retained 6 months. Records located at a Post Office are retained 3 years.
8. Overtime administrative records are retained for 7 years.
9. Tax preparation records are limited to an employee's previous year's wages, tax documentation, and health insurance coverage as required by the Affordable Care Act.

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.

System Manager(s) and Address

Chief Human Resource Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza, SW, Washington, DC 20260.

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza, SW, Washington, Dc 20260.

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

Notification Procedure

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. 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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; employees' supervisor or manager; other systems of records; claimants or their survivors or agents who make monetary claims; witnesses; investigative sources; courts; and insurance companies.

Systems Exempted From Certain Provisions of the Act

Records in this system relating to injury compensation that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 100.450
System Name:
User Profile Support Records Related to Digital Service.

System Location

Contractor sites.

Categories of Individuals Covered by the System

Current and former USPS employees and their dependents that voluntarily opt-in to use USPS Health Connect.

Categories of Records in the System

1. *User profile information:* Name, date of birth, email, gender, phone, internally assigned identifier, username, physical address, employee identification number (EIN), contact information, customer ID(s), text message number, date of account creation, method of referral to website, date of last logon, and authentication method preferences.
2. *User preferences for communications:* Frequency and channel opt in/opt out and preferred means of contact for service alerts and notifications, and language.
3. *Online user information:* Internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of first and last connection, and geographic location.
4. *Identity verification information:* username, user ID, email address, text message number, and results of identity proofing validation.

Authority for Maintenance of the System

39 U.S.C. 1003, 1004, and 1201-1209.

Purpose(s)

1. To provide administrative support to assist end users with technical questions and issues.
2. To provide account management assistance.
3. To provide account security and to deter and detect fraud.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses

Standard routine uses 1–9 and 11 apply.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and digital files.

Retrievability

For System administrators and/or customer service representatives, by internally assigned identifier, or end user account details such as name, phone number, etc. to assist end users with access/use of USPS Health Connect and to understand and fulfill end user needs.

Safeguards

Contractor site utilizes a Cloud Infrastructure under Agency Authorization to Operate (ATO) using a FedRAMP accredited Third Party Assessment Organization (3PAO) for selected Cloud Service Provider services. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All physical access to data centers by contractor employees is logged and audited routinely.

Encryption and Data Security uses Federal Information Processing Standards (FIPS) compliant encryption, secure certificates for Client and Server communication authenticity, session protection certificates for end to end protection, multiple layers of protection for data confidentiality and integrity, hashes and password storage encryption, and block level encryption for the data volumes. Customer support personnel have minimum access to user profile records.

Retention and Disposal

1. Records stored in digital service are retained until (1) the end user cancels the account, (2) six years after the end user last accesses their account, (3) until the relationship ends, or (4) after reasonable notice has been provided to the end user to export their account information in the event the agreement is terminated.
2. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

System Manager(s) and Address

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system must address inquiries in writing to the system manager. Inquiries must include full name, date of birth, physical address, email address, username, and other identifying information, if requested.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Individual end user.

USPS 100.500 System Name: Personnel Resource Management Records.

System Location

Post Offices; area and district facilities; Human Resources and Operations, Headquarters; and Computer Operations Service Centers.

Categories of Individuals Covered by the System

Current and former USPS employees.

Categories of Records in the System

1. *Employee information*: Name, Social Security Number, employee identification number(s), postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Employee resource management information:* Records related to workload, productivity, scheduling, availability, and absences, including family medical leave absences.

Authority for Maintenance of the System

39 U.S.C. 401, 404, 1001, 1003, and 1005; and 29 U.S.C. 2601 et seq.

Purpose(s)

1. To administer leave, attendance, and attendance-related awards; and to identify potential attendance problems.
2. To provide operations management with information about employee work schedules, mail volume, and productivity.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By employee name, Social Security Number, employee identification number(s), route number, duty or pay location, or pay period.

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. Restricted medical information is maintained in a separate locked cabinet under control of the FMLA Coordinator. 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.

Retention and Disposal

Resource management records related to leave application, time and attendance, and light duty status are retained 3 years. Family and Medical Leave Records are retained 5 years. Other categories of resource management records are retained 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Notification Procedure

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. 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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

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

USPS 100.600
System Name:
Personnel Research Records.

System Location

USPS Headquarters, Integrated Business Solutions Services Centers, and contractor sites.

Categories of Individuals Covered by the System

Potential applicants for USPS employment, applicants for USPS employment, USPS employee applicants for reassignment and/or promotion, employees whose work records or solicited responses are used in research projects, and former USPS employees.

Categories of Records in the System

1. Applicant, potential applicant with candidate profile, and employee information: Name, Social Security Number, Candidate Identification Number, Employee Identification Number (EIN), or respondent identification code, place of birth, postal assignment or vacancy/posting information, work contact information, home address and phone number(s), personal email address, finance number(s), duty location, and pay location.
2. Personnel research information: Records related to race, ethnicity, sex, tenure, age, veteran status, and disability status (only if volunteered by the individual); research project identifiers; and other information pertinent to personnel research.

Authority for Maintenance of the System

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

Purpose(s)

1. To support research and development efforts on personnel assessment instruments, recruitment efforts, workforce analysis, and evaluation of human resource management practices.
2. To assess the impact of selection decisions on applicants in race, ethnicity, sex, tenure, age, veteran status, and disability categories.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By individual name, Social Security Number, Candidate Identification Number, Employee Identification Number, personal email address, respondent identification code, research project identifiers, postal assignment or vacancy/posting information, duty or pay location, or location where data were collected.

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.

Retention and Disposal

Retention depends on the type of research project, but does not exceed 10 years. 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the Vice President, Employee Resource Management, 475 L'Enfant Plaza SW, Washington, DC 20260. In cases of studies involving information not collected through an examination, individuals must address inquiries to the system manager. Inquiries must contain full name; Candidate Identification Number, Employee Identification Number, or respondent identification code, and subject or purpose of research/survey; and date and location of their participation.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

USPS employees, former employees, applicants, and potential applicants with candidate profiles who provide information to personnel research programs and other systems of records.

Systems Exempted From Certain Provisions of the Act

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.

USPS 100.700 System Name: Medical Records and Related Documents.

System Location

USPS medical facilities, designee offices, and National Personnel Records Center.

Categories of Individuals Covered by the System

1. Current and former USPS employees.
2. Individuals who have been offered employment but were determined medically unsuitable or who declined the offer.
3. Current and former USPS employees who are or were required to have a commercial driver's license (CDL) or are otherwise subject to controlled substance and alcohol testing.
4. Applicants and current or former USPS employees, or persons who request reasonable accommodation on behalf of an applicant or employee.

Categories of Records in the System

1. *Employee or applicant information:* Name, Social Security Number, Employee Identification Number, Candidate Identification Number, date of birth, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Employee Medical Folder:* Restricted medical records, administrative medical records, and OWCP-related medical records.
3. *Controlled substance and alcohol testing information:* Records related to alcohol and controlled substance test results, refusals, medical review officer's evaluations, employee statements, and substance abuse professionals' evaluations and referrals.
4. *Reasonable Accommodation folders:* These folders document the decision-making process and contain records related to requests for Reasonable Accommodation.

Authority for Maintenance of the System

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

Purpose(s)

1. Medical information maintained in the employee medical folder is used to, but is not limited to, support hiring decisions and determine job-related medical suitability, fitness for duty, and Family Medical Leave Act documentation.
2. To implement a controlled substance and alcohol testing program for employees in safety-sensitive positions.
3. To provide for the uniform collection and compilation of controlled substance and alcohol test results.
4. To assess disability retirement requests.
5. To assist in making determinations about reasonable accommodation.

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. Medical records may be disclosed to an employee's private treating physician and to medical personnel retained by USPS to provide medical examinations or treatment for an employee's health or physical condition related to employment.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By employee or applicant name, Social Security Number, Employee Identification Number, Candidate Identification Number, or duty or pay location.

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.

Retention and Disposal

1. The Employee Medical Folder is retained by USPS until the employee is separated from USPS. On an annual basis, records of all employees separated during the prior year are transferred to the National Personnel Records Center and retained for 30 years.
2. Candidate medical information for applicants determined to be medically unsuitable for the position offered is retained 2 years in hard copy. Computer data is retained 3 years in a history database.
3. Documentation supporting applicant requests for reasonable accommodation for participation in the hiring or assessment process are maintained for 2 years in hard copy. Computer records of such requests are retained 3 years.
4. Reasonable Accommodation Committee and District Reasonable Accommodation Committee records are maintained for the duration of the employee's tenure with the USPS or until any appeals are adjudicated, whichever is longer. After the official use for these records has been satisfied, the records are to be placed in a sealed envelope, labeled as "Reasonable Accommodation Committee Records," and placed in the employee medical folder (EMF) and retained in accordance with the official retention period for the EMFs.

5. Alcohol test results indicating a breath alcohol concentration of 0.02 or greater, verified positive controlled substance test results, refusals, medical review officer's evaluations, employee statements, and substance abuse professionals' evaluations and referrals are retained 5 years. Alcohol test results indicating a breath alcohol concentration of less than 0.02, and negative and canceled controlled substance test results, are retained 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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 the National Medical Director, Health and Resource Management, 475 L'Enfant Plaza SW, Washington, DC 20260. Individuals who requested accommodation for an entrance examination or assessment must submit inquiries to the Manager of Selection, Evaluation, and Recognition, 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 or date of application.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees, applicants for employment; applicant or employee health care provider(s), USPS and Department of Veterans Affairs medical staff, USPS designee testing facilities, substance abuse professionals, and designated contractors.

USPS 100.800
System Name:
Employee Accident Records.

System Location

Safety offices at USPS facilities.

Categories of Individuals Covered by the System

USPS employees who sustain an on-the-job accident or an occupational injury or illness.

Categories of Records in the System

1. *Employee information*: Name, Social Security Number, Employee Identification Number, sex, age, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Accident information:* Records related to accidents and injuries such as circumstances and factors of accident or injury, statements of employee and witnesses, investigative documents, and compensation claims.

Authority for Maintenance of the System

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

Purpose(s)

1. To administer a program to collect and analyze occupational safety and health statistics.
2. To permit evaluation and correction of occupational safety and health hazards.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

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

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.

Retention and Disposal

Records are retained 5 years following the end of the calendar year of their creation. 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Employees wanting to know if information about them is maintained in this system of records 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, Room 1831, 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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; employees' supervisor or manager; witnesses; physicians; USPS accident reports; and other systems of records.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 100.850 System Name: Office of Workers' Compensation Program (OWCP) Record Copies.

System Location

USPS personnel offices.

Categories of Individuals Covered by the System

USPS employees who file for injury compensation.

Categories of Records in the System

1. *Employee information:* Name, Social Security Number, Employee Identification Number, date of birth, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Claim information:* Records and supporting information related to the claim, including copies of Department of Labor forms, postal forms and correspondence, and automated payment and accounting records.

Authority for Maintenance of the System

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

Purpose(s)

To provide injury compensation to qualifying employees, and to support USPS management decisions and requirements.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

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

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.

Retention and Disposal

Records are retained 5 years beyond the end of the calendar year in which the employee's compensation is terminated. 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Employees wanting to know if information about them is maintained in this system of records 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, Room 1831, 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.

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 266.6.

For records maintained by the Department of Labor, individuals must apply as instructed by the Department of Labor.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

For records maintained by the Department of Labor, individuals must contest records as instructed by the Department of Labor.

Record Source Categories

Employees; employees' supervisor or manager; witnesses; physicians; other systems of records, and Department of Labor.

USPS 100.900 System Name: Employee Inquiry, Complaint, and Investigative Records.

System Location

USPS personnel offices; area and district facilities; Post Offices; and contractor sites.

Categories of Individuals Covered by the System

USPS employees and non-employees who contact USPS with an inquiry or complaint, and employees and non-employees who are subjects of management inquiries or investigations of workplace issues.

Categories of Records in the System

1. *Employee information*: Name, gender, Social Security number, Employee Identification Number, postal assignment information, veteran status, contact information, finance number(s), duty location, and pay location.
2. *Non-employee information:* Name, gender, Applicant Identification Number, and contact information.
3. *Identification Number, and contact information.Inquiry, complaint, and investigative information:* Records related to the subject category of inquiry or complaint, assigned case number, background, and description of inquiry, complaint, or investigation.

Authority for Maintenance of the System

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

Purpose(s)

1. To enable review and response to inquiries and complaints concerning employees and non-employees.
2. To enable management to initiate, review, process, track, and resolve inquiries, complaints, or concerns about the workplace.
3. To support administrative or court litigation and arbitration proceedings.

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. Records may be disclosed to the National Labor Relations Board (NLRB) in response to its request for investigative purposes, to the extent that the requested information is relevant and necessary.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By employee and non-employee name, Employee Identification Number, Applicant Identification Number, subject category, facility, finance number, district, area, nationally, or case number.

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.

Retention and Disposal

Records are retained 4 years after response to inquiry, resolution of complaint, or conclusion of investigation. 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.

System Manager(s) and Address

Vice President, Employee Resource Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Notification Procedure

Employees who want to know if their information is maintained in this system of records 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. Non-employees who want to know if their information is maintained in this system of records must address inquiries to the District Manager, Human Resources that governs the facility where the inquiry, complaint, or investigative records are stored. Inquiries must include full name, address, and other identifying information. In addition, employees must include Social Security number or Employee Identification Number, name and address of facility where last employed, and dates of USPS employment. Likewise, employees may also be required to furnish where the inquiry, complaint, or investigation occurred.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees, non-employees, supervisors, managers, and witnesses.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 100.950
System Name:
Employee Assistance Program (EAP) Records.

System Location

EAP Offices at Philadelphia and Los Angeles USPS facilities. This system does not include records maintained by the supplier of EAP services as outlined in the USPS EAP contract.

Categories of Individuals Covered by the System

USPS employees and immediate family members who volunteer for or are referred to an internal EAP office at a USPS facility.

Categories of Records in the System

1. *Employee information:* Name, Social Security Number, Employee Identification Number, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Assistance information:* Case number and other personal information acquired during the period of participation.

Authority for Maintenance of the System

39 U.S.C. 401.

Purpose(s)

To provide EAP counselors with information needed to maintain program operations and to assist EAP participants.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By name, Social Security Number, Employee Identification Number, or participant case number.

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.

Retention and Disposal

Records are retained 3 years from the date of the participant's last activity. EAP contractor records are retained 7 years from the date of the participant's last activity or until litigation is resolved. 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.

System Manager(s) and Address

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

Notification Procedure

Employees wanting to know if information about them is maintained in this system of records must address inquiries to the facility head where currently, or last, employed. Inquiries must include full name, Social Security Number or Employee Identification Number, and dates of USPS employment.

For records maintained by the provider of USPS EAP services through contract, individuals must inquire as instructed by the provider.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Participating employee, other family members, and EAP counselors.

USPS 200.000 System Name: Labor Relations Records.

System Location

Labor Relations and Law Department, USPS Headquarters; EEO Compliance and Appeals Processing Centers; area and district facilities; and contractor sites.

Categories of Individuals Covered by the System

1. Current and former USPS employees, applicants for employment, third-party complainants, and mediators (other federal agency employees or contract employees) involved in EEO discrimination complaints and complaint processing.
2. USPS employees and contractors involved in labor arbitration.
3. Individuals and organizations interested in providing alternative dispute resolution (ADR) services to all disputes, except those arising under USPS collective bargaining agreements.
4. Current providers and individuals interested in providing contract investigative services for EEO complaints and contract services for drafting final agency decisions concerning EEO complaints.

Categories of Records in the System

1. *EEO discrimination complaint case information:* Individuals' names, Social Security Numbers, Employee Identification Numbers, postal assignment information, work contact information, home address(es) and phone number(s), email address(es), Veteran's Preference eligibility, finance number(s), duty location(s), pay location(s), case number, and other complaint, counseling, investigation, hearing, and appeal information describing the case.
2. *Labor arbitration information:* Records related to labor arbitration proceedings in which USPS is a party.
3. *Contractor provider information:* Records related to mediation providers, contract investigators, and contract final agency decision writers including name of individual or entity, contact information, capabilities, and performance.

Authority for Maintenance of the System

39 U.S.C. 401, 409, 410, 1001, 1005, and 1206.

Purpose(s)

1. To adjudicate complaints of alleged discrimination, and to evaluate USPS EEO program effectiveness.
2. To provide advice and representation to USPS in labor arbitration cases.
3. To determine mediation service provider, contract investigator, and final agency decision writer qualifications.

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. Records may be disclosed to the National Labor Relations Board (NLRB) in response to its request for investigative purposes, to the extent that the requested information is relevant and necessary.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

EEO discrimination complaint case records are retrieved by case number, complainant's name, Social Security Number, Employee Identification Number, or the location where the complaint was made. EEO staff selection records are retrieved by applicant name or pay location. Other records categories are retrieved by name of subject individual.

Safeguards

Paper records, computers, and computer storage media are located in secure file cabinets within locked rooms or within locked filing cabinets. Computers are maintained in offices or rooms that can be locked when users are not present and their contents are protected by user IDs and passwords. 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. 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.

Retention and Disposal

1. *EEO discrimination complaint case records:* Precomplaint records are retained 1 year after submission of a final report. Formal complaint records of closed cases are removed from the system of records quarterly, and retained as follows: Official files are retained 4 years. Copies of official files are retained 1 year. Background documents not in official files are retained 2 years. Records of closed cases on computer storage media are removed 3 years after the closure date and moved to an inactive file for future comparative analyses.
2. *Labor arbitration records:* Field-level disciplinary and contract application cases are retained 5 years from the date of final decision. National-level contract interpretation cases and court actions are retained 15 years from the date of expiration of the agreement.
3. *EEO staff selection records:* Staff selection records are retained 3 years from the date the position became vacant.

4. *ADR provider records:* Records of active providers are retained 1 year beyond the date the provider is removed from or voluntarily withdraws from the program or is otherwise notified of their decertification. Records of prospective providers who are rejected are retained 1 year beyond the year in which their survey was received.

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.

System Manager(s) and Address

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

Notification Procedure

Inquiries about EEO discrimination complaint case records regarding claims filed by field employees must be submitted to the Manager, EEO Compliance and Appeals, located in the appropriate regional office:

- Pacific and Western Areas (Region 1)
  PO Box 880546, San Francisco, CA 94188-0546;
- Southern and Great Lakes Areas (Region 2)
  PO Box 223863, Dallas, TX 75222-3863;
- Southern and Capital Metro Areas (Region 3)
  225 North Humphreys Blvd, Memphis, TN 38166-0978; and
- Eastern and Northeast Areas (Region 4)
  8 Griffin Road North, Windsor, CT 06095-1578.

Inquiries regarding claims filed by employees at Postal Service Headquarters and Headquarters Field Units and employees of the Inspection Service must be submitted to:

- Headquarters National EEO Compliance and Appeals
  475 L'Enfant Plaza NW, Washington, DC 20260-4101

Inquiries must include complainant name, complainant Social Security Number or Employee Identification Number, location, and case number and year. Inquiries about labor arbitration records mediation provider, contract investigator, and contract final agency decision writer records must be submitted to the system manager.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

For EEO discrimination complaint case information: complainants, witnesses, investigators, and respondents. For labor arbitration records: employees and other individuals involved in arbitration; counsel or other representatives for parties involved in a case; and arbitrators. For mediation provider, contract investigator, and final agency decision writer records, the service contract provider.

Systems Exempted From Certain Provisions of the Act

Pursuant to 5 U.S.C. 552a(j) and (k), USPS has established regulations at 39 CFR 266.9 that exempt EEO discrimination complaint case records. Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 300.000 System Name: Finance Records.

System Location

Computer Operations Service Centers, Integrated Business Solutions Services Centers, Accounting Service Centers, area and district facilities, personnel offices, Headquarters, Post Offices, and contractor sites.

Categories of Individuals Covered by the System

1. Debtors of USPS, including suppliers, customers, payees of money orders, and current and former employees.
2. Individuals or entities to whom USPS makes payments for materials and services received or expenses incurred in conjunction with official USPS business.

Categories of Records in the System

1. *Accounts receivable information:* Debtor's name, contact information; Social Security Number or Employee Identification Number; invoice number, other invoice or claim information, and records obtained from or disclosed to consumer reporting or credit reporting agencies.
2. *Accounts payable information:* Creditors' name, contact information; vendor identification number, tax identification number, Social Security Number, or Employee Identification Number; and other transaction details such as account, credit card, or financial institution numbers, dates, amounts, and batch numbers.

Authority for Maintenance of the System

39 U.S.C. 401, 404, 410, 1001, 1005, 1206, and 2008.

Purpose(s)

1. To facilitate debt collection by USPS.
2. To support payments to creditors of USPS.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses

Standard routine uses 1. through 10. apply. In addition:

a. Disclosure of records about USPS customers who write insufficient funds checks for USPS services may be made to the permit holder or presenter of a mailing being made on the customer's behalf. Disclosure is limited to the identity of the customer, the date of the mailing, and the date and amount of the check.

b. Disclosure of records about individuals indebted to USPS may be made to the Office of Personnel Management (OPM) under an approved computer matching program, but limited to those data elements considered relevant to determine whether the indebted individual has retirement funds available for setoff, collecting debts when funds are available for setoff, and writing off debts determined to be uncollectible.

c. Disclosure of records about individuals indebted to USPS may be made to the Defense Manpower Data Center of the Department of Defense under an approved computer matching program to identify and locate such individuals in order to initiate collection of the debts through salary and/or administrative offset procedures.

d. Disclosure of records about individuals indebted to USPS may be made to the Internal Revenue Service under an approved computer matching program to obtain the mailing address of a taxpayer in order to locate the taxpayer to collect a debt owed to USPS.

e. Disclosure of records may be made to the Department of the Treasury under Treasury Offset Program computer matching to establish the identity of a current or former Postal Service Employee as an individual owing a delinquent debt to another federal agency and to offset the salary of or payments to the employee to repay that debt.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

Accounts receivable records are retrieved by debtor name, Social Security Number, Employee Identification Number, or invoice number. Accounts payable records are retrieved by creditor name, creditor identification number, credit card number, financial institution account number, transaction date, or batch number.

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.

Retention and Disposal

Accounts receivable records are retained 3 years after the claim is paid. Accounts payable records are retained 3 years beyond the end of the fiscal year in which payment was made. 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.

System Manager(s) and Address

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

Notification Procedure

Inquiries about accounts receivable records must be submitted to the pertinent USPS facility. Inquiries about accounts payable records must be submitted to the system manager. Inquiries must include the individual's full name and tax identification number or Social Security Number.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Debtors and creditors; other systems of records; government travel card vendor; employee-designated financial institutions; and other federal agencies to which creditors have delinquent debts.

USPS 400.000 System Name: Supplier and Tenant Records.

System Location

USPS Headquarters; supply management offices; facilities service offices; and area and district facilities.

Categories of Individuals Covered by the System

Suppliers; prospective suppliers; owners and tenants of real property purchased or leased by USPS.

Categories of Records in the System

1. *Supplier information:* Records related to suppliers, such as supplier name; Social Security Number or tax identification number; business contact information; contract number; and other contract information; fingerprint cards; and experience and qualifications to provide services including principals' names and company descriptions.
2. *Real property owner and tenant information:* Records related to compensation claims by occupants of property acquired by USPS, including name and address of claimant, address of vacated dwelling, and itemized expenses.

Authority for Maintenance of the System

39 U.S.C. 401.

Purpose(s)

1. To administer contracts.
2. To determine supplier suitability for assignments requiring access to mail.
3. To adjudicate claims by owners and tenants of real property acquired by USPS.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

Individual, business, lessor, or claimant name; contract name or number, Social Security Number, tax identification number, business contact information, or address of leased facility.

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.

Retention and Disposal

1. Unsuccessful proposals and architect/ engineering questionnaires are retained 1 year beyond contract award. Contract records are closed at the end of the fiscal year in which they become inactive, and are retained 6 years thereafter.
2. Contractor fingerprint records are retained 2 years beyond contractor termination date.
3. Leased property records are closed at the end of the calendar year in which the lease or rental agreement expires or terminates, and are retained 6 years and 3 months from that date.
4. Real property owner and tenant records are retained 6 years unless required longer for litigation purposes.

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.

System Manager(s) and Address

For contracting records: Vice President, Supply Management, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For contractor fingerprint screening records: Chief Postal Inspector, Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For real property owner and tenant records: Vice President, Facilities, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the appropriate system manager. Inquiries about highway vehicle contracts must be made to the applicable USPS area office. Real property owner and tenant claimants must address inquiries to the same facility to which they submitted the claim. Inquiries must contain full individual or business name, Social Security Number, tax identification number, contract number, date of contract, or other pertinent identifying information.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Contract employees or businesses; previous dwelling owner or tenant claimant; and USPS claims reviewers and adjudicators.

USPS 500.000
System Name:
Property Management Records.

System Location

All USPS facilities.

Categories of Individuals Covered by the System

1. Individuals who are granted regular access to USPS facilities through the issuance of a building access badge, or who are assigned accountable property.
2. Individuals with authorized access to USPS computers and information resources, including USPS employees, contractors, and other individuals.
3. Individuals who are members of carpools with USPS employees or otherwise regularly use USPS parking facilities.

Categories of Records in the System

1. *Building access information:* Records related to issuance of building access badges, including name, Social Security Number, Employee Identification Number, date of birth, photograph, postal assignment information, work contact information, finance number(s), duty location, and pay location.
2. *Property issuance information:* Records related to issuance of accountable USPS property, equipment, and controlled documents, including name, Social Security Number, equipment description, equipment serial numbers, and issuance date.
3. *Computer access authorization information:* Records related to computer users, including logon ID, Social Security Number, Employee Identification Number, or other assigned identifier, employment status information or contractor status information, and extent of access granted.
4. *Identity verification information:* Question, answer, and email address.
5. *Carpool and parking information:* Records related to membership in carpools with USPS employees or about individuals who otherwise regularly use USPS parking facilities, including name, space number, principal's and others' license numbers, home address, and contact information.

Authority for Maintenance of the System

39 U.S.C. 401.

Purpose(s)

1. To ensure personal and building safety and security by controlling access to USPS facilities.
2. To ensure accountability for property issued to persons.
3. To assign computer logon IDs; to identify USPS computer users to resolve their computer access problems by telephone; and to monitor and audit the use of USPS information resources as necessary to ensure compliance with USPS regulations.
4. To authenticate user identity for the prupose of accessing USPS information systems.
5. To provide parking and carpooling services to individuals who use USPS parking facilities.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

1. Records about building access and issuance of accountable property are retrieved by name, Social Security Number, or Employee Identification Number.
2. Records about authorized access to computer and information resources are retrieved by name, logon ID, Employee Identification Number, or other unique identifier of the individual.
3. Records of carpools and parking facilities are retrieved by name, ZIP Code, space number, or parking license number.

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.

Retention and Disposal

1. Building access and accountable property records are retained until termination of access or accountability.
2. Records of computer access privileges are retained 1 year after all authorizations are cancelled.
3. Records of carpool membership and use of USPS parking facilities are retained 6 years.

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.

System Manager(s) and Address

For records of accountable property, carpool membership, and use of USPS parking facilities: Vice President, Facilities, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For records of building access and Postal Inspector computer access authorizations: Chief Postal Inspector, Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Notification Procedure

Inquiries for records about building access, accountable property, carpool membership, and use of USPS parking facilities must be addressed to the facility head. Inquiries about computer access authorization records must be directed to the Manager, Corporate Information Security, 475 L'Enfant Plaza SW, Suite 2141, Washington, DC 20260. For Inspection Service computer access records, inquiries must be submitted to the Inspector in Charge, Information Technology Division, 2111 Wilson Blvd., Suite 500, Arlington, VA 22201. Inquiries must include full name, Social Security Number or Employee Identification Number, and period of employment or residency at the location.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; contractors; subject individuals; and other systems of records.

USPS 500.050
System Name:
HSPD-12: Identity Management System (IDMS).

System Location

Records relating to the Identity Management System are maintained by a contractor at the contractor's site. This does not include building or computer access records.

Categories of Individuals Covered by the System

Individuals with authorized USPS law enforcement or emergency response duties, including postal inspectors, Office of Inspector General criminal investigators, and USPS executives and their designees.

Categories of Records in the System

1. *Cardholder information:* Records related to issuance of identity management credentials, including name, date of birth, Social Security Number (SSN), organizational and employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone number(s) as well as additional verification and demographic information. Other types of data contained in the system include federal emergency response official status; law enforcement official status; and Personal Identity Verification (PIV) Card issuance location. Records in the IDMS needed for credential management for enrolled individuals in the PIV Program includes: PIV Card serial number (all past and current Card ID numbers are retained); digital certificate(s) serial number; PIV Card issuance and expiration dates; PIV Card personal identification number (PIN); Cardholder Unique Identification Number (CHUID); and card management keys.
2. *Card-swipe records:* Records related to employees and visitors who enter and leave participating federal facilities and disaster recovery areas. This does not include direct tracking of access to USPS facilities.
3. *Computer access authorization information:* Records related to computer users, including logon ID; Social Security Number, Employee Identification Number, or other assigned identifier; employment status information; and extent of access granted.

Authority for Maintenance of the System

39 U.S.C. 401, and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

Purpose(s)

To assist in making determinations for access to other federal facilities.

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.

Storage

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

Retrievability

1. Records about building access are retrieved by name or Cardholder Unique Identifier Number.
2. Cardholder information may be retrieved by name, logon ID, or other unique identifier of the individual. Note: While many federal agencies utilize the IDMS, USPS will only have access to data on its employees enrolled in the system (not to any other agency's data).

Safeguards

All biographic and biometric data collected prior to and during the enrollment process is transmitted to the PIV IDMS over a private network in an encrypted format. Facilities and equipment are secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity. Where appropriate, this method uses the PIV card providing up to three factors of authentication. Where necessary, this method also consists of two components (e.g., user ID + password). Physical security measures are employed to protect enrollment equipment, facilities, material, and information systems, including locks, ID badges, fire protection, redundant power and climate control to protect IT equipment. The PIV IDMS sends confirmed enrollment information to the card production facility via a secure FTP connection. Cards that are not active cannot be used for access to federal facilities. Certifications are revoked when they are reported lost, stolen, damaged beyond use, or when a cardholder has failed to meet the terms and conditions of enrollment. Cards will be deactivated upon collection of damaged cards or if the employee no longer requires a PIV card.

Retention and Disposal

1. Building access records are retained according to the policies of the agencies visited.
2. Records of computer access privileges and authorization information are retained 5 years after the cardholder is separated from the Postal Service.

Data will be disposed of according the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 Guidelines for Media Sanitization. Magnetic media will be degaussed and then destroyed; paper records will be stored in locked bins, transported securely via bonded courier, and shredded.

System Manager(s) and Address

For collection of cardholder information: Chief Postal Inspector, United States Postal Inspection Service, 475 L'Enfant Plaza SW Fl 3, Washington, DC 20260.

For records relating to the Identity Management System and identification cards: Program Manager, HSPD-12 Managed Service Office, Federal Acquisition Service (FAS), General Services Administration, 10304 Eaton Place Fl 3, Fairfax, VA 22030.

For records of building access to other federal buildings, contact that agency.

Notification Procedure

Inquiries for records about building access must be addressed to the facility head. Inquiries about access to the IDMS are to be directed to the Program Manager, HSPD-12 Managed Service Office, Federal Acquisition Service (FAS), General

Services Administration, 10304 Eaton Place Fl 3, Fairfax, VA 22030. Inquiries regarding collection of cardholder information are to be directed to the Chief Postal Inspector, United States Postal Inspection Service, 475 L'Enfant Plaza SW Fl 3, Washington, DC 20260. Inquiries must include full name, Social Security Number or Employee Identification Number, and period of employment or residency at the location.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees, subject individuals, former employers, and other systems of records.

USPS 500.100
System Name:
Carrier and Vehicle Operator Records.

System Location

Headquarters; area and district facilities; processing and distribution centers; bulk mail centers; vehicle maintenance facilities; Post Offices; Integrated Business Solutions Services Centers; Accounting Service Centers; contractor or licensee locations; and facilities employing persons under a highway vehicle contract.

Categories of Individuals Covered by the System

1. City letter carriers.
2. Current and former USPS employees who operate or maintain USPS-owned or leased vehicles.
3. Contract highway vehicle operators.

Categories of Records in the System

1. *Carrier information:* Records related to city letter carriers, including carrier's name, Social Security Number, Employee Identification Number, age, postal assignment information, work contact information, finance number(s), duty location, pay location, route number and work schedule, and effective date of agreement for use of a privately owned vehicle to transport the mail, if applicable.
2. *Vehicle operator information:* Records of employees' operation or maintenance of USPS-owned or leased vehicles, including employee name, Social Security Number, Employee Identification Number, age, postal assignment information, work contact information, finance number(s), duty location, pay location, work schedule, vehicle operation licensing and driving records, and other records of vehicle operation and maintenance.
3. *Highway vehicle contract employee information:* Records related to contract employee name, Social Security Number, date and place of birth, address and employment history, driver's license number, and contract assignment information.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, and 1206.

Purpose(s)

1. To reimburse carriers who use privately owned vehicles to transport the mail pursuant to a postmaster agreement.
2. To evaluate delivery and collection operations and to administer these functions.
3. To provide local Post Office managers, supervisors, and transportation managers with information to assign routes and vehicles, and to adjust workload, schedules, and type of equipment operated.
4. To determine contract vehicle operator suitability for assignments requiring access to mail.
5. To serve as a basis for vehicle operator corrective action and presentation of safe driving awards.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name, Social Security Number, Employee Identification Number, pay location, Postal Service facility name, route number, or vehicle number.

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.

Retention and Disposal

1. Route inspection records and minor adjustment worksheets are retained 2 years where inspections or minor adjustments are made annually or more frequently. Where inspections are made less than annually, records are retained until a new inspection or minor adjustment, and an additional 2 years thereafter.
2. Statistical engineering records are retained 5 years, and may be retained further on a year-to-year basis.
3. Agreements for use of a privately owned vehicle are retained 2 years. Post office copies of payment authorizations are retained 90 days.
4. Records of employees who operate or maintain USPS vehicles are retained 4 years.
5. Records of highway vehicle contract employees are retained 1 year after contract expiration or contract employee termination.

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.

System Manager(s) and Address

Vice President, Delivery and Post Office Operations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Current and former employees, and highway vehicle contract employees, wanting to know if information about them is

maintained in this system of records must address inquiries to the facility head where currently or last employed. Requests must include full name, Social Security Number or Employee Identification Number, and, where applicable, the route number and dates of any related agreements or contracts.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; contractors; carrier supervisors; route inspectors; and state motor vehicle departments.

USPS 500.200
System Name:
Controlled Correspondence, FOIA, and Privacy Act Disclosure Records.

System Location

Postmaster General, Government Relations, and Consumer and Industry Affairs offices, Headquarters; Office of the Inspector General, Law Department, Headquarters and field offices; records custodian offices at USPS Headquarters and field offices.

Categories of Individuals Covered by the System

1. Individuals who correspond directly with the Office of the Postmaster General.
2. Individuals who have written to non-USPS government officials; congressmen and other government officials who write USPS on behalf of USPS customers, employees, or other individuals; and individuals to whom USPS announcements or greetings are regularly directed.
3. Individuals who submit inquiries and requests for information or records, including under the FOIA.
4. Individuals who submit inquiries or requests for information or records, or who contest a record, subject to the provisions of the Privacy Act and privacy complaints.
5. Individuals whose information is covered by a system of records that has been disclosed outside of the Postal Service.

Categories of Records in the System

1. *Correspondence information:* Records related to controlled correspondence including correspondent's name, address, nature of inquiry, response, and original correspondence. May include referral letters, e-mail correspondence, internal memoranda, logs/notes of USPS staff and other related material.
2. *Records Inquiries:* Records related to individuals who request information, including under the FOIA or the Privacy Act, or who request amendment of a record, including name, Social Security Number, date of birth, nature of inquiry, original correspondence, response, and records from other systems of records compiled in response to the inquiry. May also include referral letters, e-mail correspondence, internal memoranda, logs/notes of USPS staff and other related material. These files may also contain information or determinations furnished by and correspondence with other Federal agencies.
3. *General Inquiries:* Records related to inquiries or complaints concerning Postal Service records including correspondent's name, address, nature of inquiry, response, and original correspondence. May include referral letters, e-mail correspondence, internal memoranda, logs/notes of USPS staff and other related material.
4. *Accounting of disclosure records*: The date, nature, and purpose of each disclosure of a Privacy Act covered record to any person or to another agency and the name and address of the person or agency to whom the disclosure is made.

Authority for Maintenance of the System

39 U.S.C. 401, 410, and 412. 5 U.S.C. 552, as amended, 5 U.S.C. 552(a).

Purpose(s)

1. To maintain correspondence files for persons who communicate with the Office of the Postmaster General, and correspondence from other government officials.
2. To respond to inquiries or complaints concerning Postal Service records and to requests for records and information, including FOIA and Privacy Act requests, and to comply with FOIA and Privacy Act disclosure accounting and reporting requirements. The records are also used to facilitate the preparation of statistical and other reports regarding use of the FOIA.
3. To comply with Privacy Act accounting of disclosure requirements.

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. Records may be provided to a federal agency, when that agency may maintain records relevant to a Privacy Act or FOIA request, for that agency's disclosure determination, or to obtain its assistance on a USPS disclosure determination.
b. Records may be provided to the Office of Government Information Services for the purpose of resolving disputes between FOIA requesters and Federal agencies, including the Postal Service, and reviewing Postal Service policies, procedures, and compliance in order to recommend policy changes to Congress and the President.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

1. Correspondence records are retrieved by subject category, by the individual's name, or by the name of the official inquiring on his or her behalf.
2. FOIA and Privacy Act disclosure records are retrieved by case number, name of the requester, or the name of the attorney or agent acting on their behalf.
3. Accounting of disclosure records are retrieved by the name of the record's subject.

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.

Retention and Disposal

Correspondence records are retained 4 years. FOIA and Privacy Act-related records are cut off at the end of each fiscal or calendar year, respectively, and retained 6 years thereafter. Accounting of disclosure records are retained for five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made. 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.

System Manager(s) and Address

For Postmaster General correspondence: Office of the Postmaster General, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For FOIA and Privacy Act requests: General Counsel and Executive Vice President, 475 L'Enfant Plaza SW, Washington DC 20260.

For other correspondence in this system: Vice President, Government Relations and Public Policy, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager. Inquiries about Office of the Postmaster General correspondence must include the full name of the originator, date, and subject of correspondence. Inquiries about other kinds of correspondence must contain the full name of the originator, the name of the government official to whom written, if applicable, and the date of the correspondence. Inquiries about FOIA and Privacy Act disclosure accounting records must contain the individual's name, or that of their agent, and the date of the request.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Individuals who submit correspondence, FOIA, or Privacy Act requests; their counsel or other representative; USPS officials who prepare responses; and other systems of records.

Systems Exempted From Certain Provisions of the Act

Records in this system related to FOIA and Privacy Act inquiries that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 500.300
System Name:
Emergency Management Records.

System Location

Headquarters and all field postal facilities.

Categories of Individuals Covered by the System

1. USPS employees and other individuals having emergency management responsibilities officially designated by the Postal Service to mitigate, prepare for, respond to, or recover from any natural disaster or manmade hazard.
2. Household members of USPS employees and other individuals having emergency management responsibilities officially designated by the Postal Service to mitigate, prepare for, respond to, or recover from any natural disaster or manmade hazard.
3. Individuals who are evacuees from postal facilities or who are unaccounted for in the event of a natural disaster or manmade hazard affecting a postal facility.
4. Individuals whose names have been provided to the Postal Service by government agencies or disaster relief organizations as a result of a disaster or manmade hazard.

Categories of Records in the System

1. *Emergency management information:* Records related to USPS employees and contractors having officially designated emergency management responsibilities, including: name; Social Security Number or Employee Identification Number; date of birth; postal or contract assignment information; home, work, and emergency contact information; duty location, work schedule; and assigned emergency management devices.
2. *Medical fitness and surveillance information:* Records related to medical documentation such as receipt of prophylaxis, tests, including determinations of fitness to wear protective equipment, and surveillance for exposure to hazards.
3. *Emergency management training information:* Records related to specialized training in emergency management of natural disasters and manmade hazards completed by emergency management personnel.
4. *Evacuee information:* Records of individuals who are impacted by natural disasters or manmade hazard, such as name; postal assignment information (if USPS employee); home, work, and emergency contact information; home and work address; location in facility and activities prior to evacuation; route of exit from facility; rallying point; and emergency medical treatment administered to evacuees.

Authority for Maintenance of the System

39 U.S.C. 401 and 410.

Purpose(s)

1. To permit collaboration among officially designated individuals who are responsible for mitigation of, preparation for, response to, and recovery from any natural disaster or manmade hazard involving the Postal Service.
2. To satisfy federal requirements for the training, fitness testing, and medical surveillance of individuals in response to a natural disaster or manmade hazard involving the Postal Service.
3. To test for the exposure of individuals to hazards.
4. To account for the whereabouts of individuals in response to a natural disaster or manmade hazard at a postal facility.
5. To assess the likelihood of an individual's exposure to a hazard and to contact the individual with important health-related information.
6. To provide information about disaster recovery programs and services to individuals affected by a natural disaster or manmade hazard.

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.

a. Medical records may be disclosed to an individual's private treating physician, to medical personnel retained by USPS, and to public health agencies to provide medical examinations, medications, or treatment to individuals covered by this system of records.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name, Social Security Number, Employee Identification Number, and postal facility name.

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.

Retention and Disposal

1. Emergency management information and emergency management training information is retained 5 years beyond the end of the period for which the individual is assigned emergency management responsibilities.
2. Medical documentation including fitness and medical surveillance information is retained 30 years from the date of collection.
3. Evacuee information is retained 5 years from the date of collection.

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.

System Manager(s) and Address

Chief Postal Inspector, United States Postal Inspection Service, United States Postal Service, 475 L'Enfant Plaza S.W., Washington, DC 20260.

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

Senior Director, Office of the Postmaster General and CEO, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Manager, Safety, Security, Emergency Planning, United States Postal Service Office of Inspector General, 1735 N. Lynn Street, Arlington, VA 22209.

Notification Procedure

Current and former employees and contractors wanting to know if information about them is maintained in this system of records must address inquiries to the facility head where currently or last employed. Headquarters employees or contractors must submit inquiries to the chief postal inspector. Requests must include full name, Social Security Number or Employee Identification Number, and employment or contract dates. Individuals from whom evacuee information may have been collected must address inquiries to the head of the facility from which they were evacuated. Household members of current or former field employees and other individuals having emergency management responsibilities officially designated by the Postal Service must address inquiries to the facility head where the postal employee in their household is currently or was last employed. Household members of current or former Headquarters employees and other individuals having emergency management responsibilities officially designated by the Postal Service must submit inquiries to the Chief Postal Inspector.

Record Access Procedures

Employees; contractors; medical staff of the Postal Service; designated contractors; public health agencies; emergency response agencies, providers, first responders; individuals who are evacuated in the event of a natural disaster or manmade hazard; and household members of USPS employees and other individuals having emergency management responsibilities officially designated by the Postal Service.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Employees; contractors; medical staff of the Postal Service; designated contractors; public health agencies; emergency response providers, first responders; individuals who are evacuated in the event of a natural disaster or manmade hazard; and household member of USPS employees and other individuals having emergency management responsibilities officially designated by the Postal Service.

Systems Exempted From Certain Provisions of the Act

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.

USPS 600.000
System Name:
Legal Records Related to Mail.

System Location

Law Department, USPS Headquarters and field offices; Prohibitory Order Processing Center (POPC).

Categories of Individuals Covered by the System

1. Complainants, respondents, and opposing parties in cases of false representations, lotteries, or nonmailable matter; prohibitory orders; mail withheld from delivery; and denial or termination of Post Office box or caller service.
2. USPS attorneys, attorneys representing parties, subjects of investigations, and postal inspectors involved in such cases.
3. Addressees who request orders prohibiting further mailings to them by mailers of pandering advertisements, and the mailers against whom such orders are issued.

Categories of Records in the System

1. *False representation, mailability, and lotteries information:* Records related to administrative proceedings and litigation involving false representation, mailability, and lotteries, including names of involved individuals.
2. *Prohibitory order information:* Applications for prohibitory orders, issued orders, applications for order enforcement, complaints issued to alleged violators, and notices of court action, including names of involved individuals.
3. *Withholding of mail information:* Records related to the withholding of mail from delivery, including names of involved individuals.
4. *Denial or termination of Post Office box or caller service information:* Records related to the denial or termination of a Post Office box or caller service, including names of involved individuals.

Authority for Maintenance of the System

39 U.S.C. 204, 401, 404, and 3001 et seq.; 18 U.S.C. 1301, 1302, 1341, and 1342.

Purpose(s)

1. To investigate and enforce USPS statutes about false representations, lotteries, and mailability.
2. To process applications for orders prohibiting mailers of pandering advertisements from making further mailings to the applicants, to determine whether violations of such orders have occurred, and to prevent them.
3. To enable representation of USPS in administrative proceedings when customers petition for review of cases in which USPS has withheld mail from delivery or refused or terminated Post Office box or caller service.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By individual name, USPS docket number, or prohibitory order number.

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.

Retention and Disposal

1. Records about false representations, lotteries, or nonmailable matter through the mails are retained 20 years.
2. Records about prohibitory orders against pandering advertisers are retained 5 years following issuance of order or last application for enforcement.
3. Records about an appeal of withholding of mail are retained 1 year after final disposition of the case.
4. Records about refusal to provide, or involuntary termination of, Post Office box or caller service are retained 1 year after final disposition of the case.

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.

System Manager(s) and Address

General Counsel and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager, and provide the following information: the full name of the subject individual; and, if applicable, the names of respondents, appellants, plaintiffs, attorneys or agents; and dates of appeals, filings, or proceedings.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject individuals; their counsel or other representative; postal inspectors; Prohibitory Order Processing Center personnel; members of the Judicial Officer Department; attorneys for USPS; attorneys for mailers; witnesses; and postmasters.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 600.100
System Name:
General Legal Records.

System Location

Law Department, USPS Headquarters and field offices; area and district facilities; Integrated Business Solutions Services Centers; Tort Claims Center; and Post Offices.

Categories of Individuals Covered by the System

1. Current or former USPS employees who are parties to National Labor Relations Board (NLRB) cases, or on whose behalf NLRB charges are filed by a collective bargaining representative, and other individuals involved in labor or employment litigation.
2. Individuals who claim to be involved in accidents related to USPS operations and who seek money damages under the Federal Tort Claims Act.
3. Individuals investigated for possible infringement of USPS intellectual property rights, including inventors seeking patents for devices.
4. Individuals involved in other formal administrative proceedings or litigation in which USPS is a party or has an interest in which information or testimony is sought.

Categories of Records in the System

Records related to proceedings, including individuals' names, Social Security Numbers, postal assignment information, work contact information, finance number(s), duty location, pay location, assigned case or docket numbers, and other details related to the nature of the litigants and litigation subject matter.

Authority for Maintenance of the System

39 U.S.C. 401, 409, 1206, and 1208.

Purpose(s)

1. To provide legal advice and representation in NLRB cases, labor or employment litigation, and miscellaneous civil actions and litigation.
2. To consider, settle, or defend against tort claims made under the Federal Tort Claims Act; to support program management by accident prevention and safety officers; and to provide pertinent information regarding safety, accidents, and claims to equipment providers and insurers.
3. To protect USPS intellectual property and patents.

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. Tort claims records may be disclosed to members of the American Insurance Association Index System; to insurance companies that have issued policies under which the United States is or may be an (additional) insured; to equipment manufacturers, suppliers, and their insurers for claims considerations and possible improvement of equipment and supplies; and in response to a subpoena or other appropriate court order.

b. A record may be transferred and information from it disclosed to the Patent and Trademark Office or the Library of Congress when relevant in any proceeding involving the registration of Postal Service trademarks or issuance of patents.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name of subject individual, litigant, claimant, charging party, or individual on whose behalf a charge has been filed; case number, docket number, or topic title.

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.

Retention and Disposal

1. Labor litigation records are retained 5 years.
2. Tort claim files are retained 7 years after final adjudication or other closure. Tort litigation files are retained 5 years after closure.
3. Records of investigations of possible infringement of USPS intellectual property rights are retained 25 years after closure of the case.
4. Records of miscellaneous civil actions and administrative proceedings are retained 10 years.

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.

System Manager(s) and Address

General Counsel and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager. Inquiries must include full name of litigant, charging party, or individual on whose behalf a charge has been filed, case number or docket number, if known, and the approximate date the action was instituted.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject individuals; their counsel or other representative; external authorities such as the NLRB, Equal Employment Opportunity Commission, or Merit System Protection Board; customers; police; postal inspectors; witnesses; American Insurance Association Index reports; and other systems of records.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 600.200 System Name: Privacy Act and FOIA Appeal and Litigation Records.

System Location

Law Department, USPS Headquarters.

Categories of Individuals Covered by the System

Individuals who submit administrative appeals or bring suit against USPS under the provisions of the Privacy Act of 1974 and/or FOIA.

Categories of Records in the System

Names, Social Security Numbers, dates, case numbers, and other information related to individuals and the subject matter of the appeal and/or litigation.

Authority for Maintenance of the System

39 U.S.C. 401, 409, 410, and 412.

Purpose(s)

To process appeals, assist in litigation, and comply with reporting requirements related to the Privacy Act and FOIA.

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. Records may be provided to a federal agency, when that agency may maintain records relevant to a Privacy Act or FOIA request, for that agency's disclosure determination, or to obtain its assistance on a USPS disclosure determination.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By case number, name of requester, or name of their attorney or agent.

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.

Retention and Disposal

Records are retained 10 years. 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.

System Manager(s) and Address

General Counsel and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager, and provide the following information: the name of the individual or agent who submitted the appeal, and the year in which the appeal was made, or, if applicable, the name of the plaintiff in the civil action and the year in which the civil action was filed.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject individuals; their counsel or other representative; USPS officials; other agencies referring requests to USPS; and other systems of records.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 600.300 System Name: Public and Confidential Financial Disclosure Reports.

System Location

USPS Headquarters, Ethics Office.

Categories of Individuals Covered by the System

Employees required to file public or confidential financial disclosure reports, including the Postmaster General, Deputy Postmaster General, USPS Chief Ethics Officer, administrative law judges, the Governors of the Postal Service, and other USPS employees determined by regulation.

Categories of Records in the System

1. *Public Financial Disclosure Report:* Standard Form OGE Form 278 and supplemental statements including the individual's name, title, work location, employment status, personal financial records, and reports related thereto.
2. *Executive Branch Personnel Confidential Financial Disclosure Report:* Office of Government Ethics. OGE Form 450 and supplemental statements including the individual's name, title, work location, employment status, personal financial records, and reports related thereto.

Authority for Maintenance of the System

39 U.S.C. 401, 410; and 5 U.S.C. Appendix 4.

Purpose(s)

To meet the statutory requirements of the Ethics in Government Act with respect to the filing of public and confidential financial disclosure reports by covered individuals.

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. Records may be disclosed to any source when necessary to obtain information relevant to a conflict-of-interest investigation or determination.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By individual's name.

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.

Retention and Disposal

Records are retained 6 years. 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.

System Manager(s) and Address

Ethics Office, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries as follows:

For all OGE Form 450 filers, to the Ethics Office, USPS Headquarters.

For field and Headquarters OGE Form 278 filers, to the system manager.

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 266.6. Requests for OGE Form 278 reports must be submitted using OGE Form 201.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject individual; their counsel or representative; ethics officials; individuals alleging conflicts of interest; and persons contacted during any investigation of such allegations.

USPS 600.400 System Name: Administrative Litigation Records.

System Location

Law Department, USPS Headquarters; area and district facilities; and USPS facilities.

Categories of Individuals Covered by the System

1. Current and former USPS employees involved in MSPB appeals.
2. USPS employees and applicants for employment involved in EEO litigation.

Categories of Records in the System

Records related to individuals involved in MSPB appeals or EEO litigation, including names, Social Security Numbers, Employee Identification Numbers, work locations, dates, case number, and other information related to the litigants and the subject matter of the litigation.

Authority for Maintenance of the System

39 U.S.C. 401 and 409.

Purpose(s)

To provide advice and representation to USPS in MSPB appeals and EEO litigation.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name of litigant or case number.

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.

Retention and Disposal

MSPB appeals records are retained 7 years from the date of the last administrative or judicial decision. EEO litigation records are retained 4 years from the date of the final decision. 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.

System Manager(s) and Address

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

General Counsel and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager, and provide full name, case number, if known, and the approximate date the action was instituted.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject employees; counsel or other representatives for parties; and other individuals involved in appeal or litigation.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 600.500 System Name: Judicial Officer Records

System Location

Judicial Officer Department, USPS Headquarters Library

Categories of Individuals Covered by the System

Persons identified in proceedings before, and decisions of, the U.S. Postal Service Judicial Officer Department; including complainants, respondents, petitioners, and disputants and their representatives.

Categories of Records in the System

1. *Initial and Final Decisions Provided for public posting on usps.com:* Initial and Final Decisions that have been reviewed for inclusion of Social Security Numbers or equivalent non-publicly-available personally identifiable information and redacted as required before being furnished for posting and public availability on the U.S. Postal Service public website, *usps.com*.
2. *Judicial Officer Department Administrative Decision-related information:* Records related to persons identified as parties (or their representatives) in published Judicial Officer Administrative Decisions, including name and such information as: date of birth, Social Security Number (SSN), Employee Identification Number, organizational and employee affiliations, work-related and/or personal mailing addresses, e-mail addresses, and phone number(s) as well as additional identity verification information.
3. *Judicial Officer Department Administrative Proceedings-related information:* Records related to persons identified as parties (or their representatives) in Judicial Officer proceedings that do not lead to published decisions, including name and such information as: date of birth, Social Security Number (SSN), Employee Identification Number, organizational and employee affiliations, work-related and/or personal mailing addresses, e-mail addresses, and phone number(s) as well as additional identity verification information; details of circumstances described in the proceedings documentation, including business names, addresses, activities, and any relevant or explanatory details provided to the Judicial Officer Department.

Authority for Maintenance of the System

39 U.S.C. 204; 39 C.F.R. 951, 952, 953, 954, 957, 958, 959, 960, 961, 962, 963, 964, 965, and 966.

Purpose(s)

1. To enable USPS Judicial Officer Department Administrative proceedings.
2. To make Initial and Final USPS Judicial Officer Department Administrative Decisions available to the public.

Routine Uses of Records Maintained In the System, Including Categories of Users and the Purposes of Such Uses

Standard routine uses 1. through 11. apply.

a. Initial and Final Judicial Officer Department Administrative Decisions are made available to the public (after redaction of Social Security Numbers or equivalent non-publicly-available personally identifiable information) on the U.S. Postal Service public website, *usps.com*.

b. Records provided in the course of litigation at the request of any party to a pending or completed proceeding are considered Disclosures Incident to Legal Proceedings.

c. Records presented or displayed or otherwise disclosed during the course of a public hearing conducted in connection with any Judicial Officer Department are considered Disclosures Incident to Legal Proceedings. Requests can be made that any specifically confidential records be reviewed only in camera and kept under seal.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Initial and Final USPS Judicial Officer Department Administrative Decisions are stored in online formats on *usps.com*.

Retrievability

By individual name, USPS docket number; or by USPS designation of applicable 39 USC Part number; Initial and Final USPS Judicial Officer Administrative Decisions (after redaction of Social Security Numbers or equivalent non-publicly-available personally identifiable information) may be retrieved on *usps.com* by year, party name, docket number, or by use of full text searches.

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. Unsupervised access to records is limited to individuals whose official duties require such access. 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.

Retention and Disposal

1. Judicial Officer Department Administrative Proceedings records are retained for 20 years.
2. Judicial Officer Initial and Final Administrative Decisions are retained indefinitely.
3. Initial and Final Administrative Decisions furnished for posting and public availability on the U.S. Postal Service public website, *usps.com*, are retained indefinitely.

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.

System Manager(s) and Address

Judicial Officer, United States Postal Service, 2101 Wilson Boulevard, Suite 600, Arlington, VA 22201-3078.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager, and provide the following information: the full name of the subject individual; and, if applicable and known, the names of complainants, respondents, petitioners, disputants, and/or their representatives, and the dates of decisions, or proceedings.

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 266.6.

Contesting Record Procedure

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subject individuals; their counsel or other representatives; postal inspectors; Prohibitory Order Processing Center personnel; members of the Judicial Officer Department; attorneys for USPS; attorneys for mailers; witnesses; postmasters; and persons identified in proceedings and decisions of the U.S. Postal Service Judicial Officer Department.

Systems Exempted From Certain Provisions of the Act

Records in this system that have been compiled in reasonable anticipation of a civil action or proceeding are exempt from individual access as permitted by 5 U.S.C. 552a(d)(5). 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.

USPS 700.000 System Name: Inspection Service Investigative File System.

System Locations

Office of the Chief Postal Inspector, USPS Headquarters; Inspection Service Human Resources Service Center, Security Investigation Service Center, and Criminal Investigation Service Center; Inspectors-in-Charge.

Categories of Individuals Covered by the System

1. Subjects of investigations; complainants, informants, witnesses, and other individuals in investigations.
2. Applicants, current and former USPS employees, contractors, and other individuals providing information related to employment suitability checks.
3. Applicants for and appointees to sensitive positions in USPS, and individuals providing information related to security clearance checks on those individuals.

Categories of Records in the System

Records related to investigations, including person name(s), Social Security Number(s), case number, addresses, reports of postal inspectors and third parties; physical identifying characteristics (including fingerprints, voiceprints, handwriting samples, polygraph tests, photographs, or other biometrics); and employment and payroll information maintained by USPS.

Authority for Maintenance of the System

39 U.S.C. 401 and 404; and 18 U.S.C. 3061.

Purpose(s)

To support investigations of criminal, civil, or administrative matters, including applicant, employee, and contractor background investigations.

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. A record from this system may be disclosed to the public, news media, trade associations, or organized groups to provide information of interest to the public about the activities and the accomplishments of USPS or its employees.

b. A record relating to a person held in custody pending or during arraignment, trial, sentence, or extradition proceedings or after conviction may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual involved with the maintenance, transportation, or release of such a person.

c. A record relating to a case or matter may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, under an international treaty, convention, or executive agreement; or to the extent necessary to assist such country in apprehending or returning a fugitive to a jurisdiction that seeks that individual's return.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name or other personal identifier, subject category, or assigned case number.

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.

Retention and Disposal

Records are retained up to 15 years. Exceptions may be granted for longer retention in specific instances. 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.

System Manager(s) and Address

Chief Postal Inspector, Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager and include full name, address, and information sufficient to ascertain the investigation and the individual's involvement.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subjects, applicants, applicant references, employees, complainants, witnesses, other systems of records, other government agencies, and external public or private sources.

Systems Exempted From Certain Provisions of the Act

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.

USPS 700.100 System Name: Mail Cover Program Records.

System Location

Chief Postal Inspector, USPS Headquarters; Criminal Investigation Service Center; Inspection Service field offices.

Categories of Individuals Covered by the System

Individuals on whom a mail cover has been duly authorized by USPS to obtain information in the interest of (a) protecting the national security; (b) locating a fugitive; and (c) obtaining evidence of the commission or attempted commission of a crime that is punishable by imprisonment for a term exceeding 1 year.

Categories of Records in the System

Records related to names and addresses of individuals on whom a mail cover is authorized; interoffice memoranda and materials; and correspondence with other relevant agencies.

Authority for Maintenance of the System

39 U.S.C. 401 and 404.

Purpose(s)

To investigate the commission of, or attempted commission of, acts constituting a crime punishable by law.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By subject individual name.

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.

Retention and Disposal

Records are retained 5 years. 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.

System Manager(s) and Address

Chief Postal Inspector, Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager. Inquiries must include full name of subject individual, current address, and other addresses during the previous 5 years.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

The requesting authority and postal inspectors.

Systems Exempted From Certain Provisions of the Act

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.

USPS 700.200
System Name:
Vehicular Violations Records System.

System Location

Inspection Service, USPS Headquarters; and USPS facilities where postal police officers issue vehicular violations notices.

Categories of Individuals Covered by the System

Vehicle operators.

Categories of Records in the System

Vehicle operator's and postal police officers' names; operator's state permit and permit number; state vehicle license number; date, number, and cause of citation; and dates of court appearances.

Authority for Maintenance of the System

39 U.S.C. 401.

Purpose(s)

To regulate traffic and parking on USPS premises.

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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper

Retrievability

By the subject individual name or vehicle license number.

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.

Retention and Disposal

Vehicular violations records are retained 2 years. 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.

System Manager(s) and Address

Chief Postal Inspector, Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260

Notification Procedure

Individuals at USPS Headquarters wanting to know if information about them is maintained in this system of records must address inquiries to: Inspector-in-Charge for Internal Affairs, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260. Individuals at other facilities must address inquiries to the facility's Inspector-in-Charge.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Vehicle operators; postal police officers; witnesses; state motor vehicle registration bureaus; USPS personnel offices; USPS parking control officers; prosecutive and judicial officials; and other systems of records.

USPS 700.300 System Name: Inspector General Investigative Records.

System Location

Office of the Inspector General (OIG), USPS Headquarters; OIG field offices.

Categories of Individuals Covered by the System

1. Present and former USPS employees and applicants for employment, contractors, subcontractors, lessees, licensees, and other persons who are named individuals in investigations conducted by OIG or who are subjects of security checks or suitability determinations.
2. Complainants and subjects of complaints collected through the operation of the OIG Hotline.
3. Other individuals, including witnesses, sources, and members of the general public, who are named individuals in connection with investigations conducted by OIG.

Categories of Records in the System

Records related to OIG investigations, including name(s), Social Security Number(s), assigned case number, addresses; reports of OIG investigators and third parties; investigative materials; physical identifying characteristics (including fingerprints, voiceprints, handwriting samples, polygraph tests, photographs, or other biometrics); and employment, payroll, financial, contractual, and property management records maintained by USPS.

Authority for Maintenance of the System

39 U.S.C. 404; 18 U.S.C. 3061; and 5 U.S.C. Appendix 3.

Purpose(s)

To support the conduct of OIG investigations.

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. A record from this system may be disclosed to the public, news media, trade associations, or organized groups to provide information of interest to the public about the activities and the accomplishments of USPS or its employees.

b. A record relating to a person held in custody pending or during arraignment, trial, sentence, or extradition proceedings or after conviction may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual involved with the maintenance, transportation, or release of such a person.

c. A record relating to a case or matter may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, under an international treaty, convention, or executive agreement; or to the extent necessary to assist such country in apprehending or returning a fugitive to a jurisdiction that seeks that individual's return.

d. Records originating exclusively within this system of records may be disclosed to other federal offices of inspector general and councils comprised of officials from other federal offices of inspector general, as required by the Inspector General Act of 1978, as amended. The purpose is to ensure that OIG audit and investigative operations can be subject to integrity and efficiency peer reviews, and to permit other offices of inspector general to investigate and report on allegations of misconduct by senior OIG officials as directed by a council, the President, or Congress. Records originating from any other USPS systems of records, which may be duplicated in or incorporated into this system, may also be disclosed with all personally identifiable information redacted.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By name or other personal identifier, subject category, or assigned case number.

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.

Retention and Disposal

1. Official investigative case files, evidence and custody files, and informant files are retained up to 20 years, or 5 years beyond the sentence of the subject individual, whichever is longer.
2. Information reports, investigative analysis reports, confidential fund files, and inspection reports are retained 5 years.
3. Proactive project case files and briefing reports are retained 2 years after closeout.

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.

System Manager(s) and Address

Inspector General, United States Postal Service, 1735 N Lynn Street, Arlington, VA 22209.

Notification Procedure

Individuals wanting to know if information about them is maintained in this system of records must address inquiries to the system manager and include full name, address, and information sufficient to ascertain the investigation and the individual's involvement.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Subjects, applicants, applicant references, employees, complainants, witnesses, other systems of records, other government agencies, and external public or private sources.

Systems Exempted From Certain Provisions of the Act

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.

USPS 800.000 System Name: Address Change, Mail Forwarding, and Related Services.

System Location

USPS National Customer Support Center (NCSC), Computerized Forwarding System (CFS) sites, Post Offices, USPS Processing and Distribution Centers, USPS IT Eagan Host Computing Services Center, and contractor sites.

Categories of Individuals Covered by the System

Customers requesting change of address, mail forwarding, or other related services either electronically or in writing. Customers who are victims of a natural disaster who request mail forwarding services through the Postal Service or the American Red Cross.

Categories of Records in the System

1. *Customer information:* Name, title, signature, customer number, old address, new address, filing date, email address(es), telephone numbers, and other contact information.
2. *Verification and payment information:* Credit and/or debit card number, type, and expiration date; or date of birth and driver's state and license number; information for identity verification; and billing information. Customers who are victims of a natural disaster who request mail forwarding service electronically may be required to provide date of birth for verification if credit and/or debit card information is unavailable.
3. *Demographic information:* designation as individual/family/business.
4. *Customer preferences:* Permanent or temporary move; mail forwarding instructions; service requests and responses.
5. *Customer inquiries and comments:* Description of service requests and responses.
6. *Records from service providers* for identity verification.
7. *Online user information:* Internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of connection, and geographic location.
8. *Protective Orders.*

Authority for Maintenance of the System

39 U.S.C. 401(2), 403, and 404(a)(1).

Purpose(s)

1. To provide mail forwarding and change of address services, including local community information, and move related advertisements.
2. To provide address correction services.
3. To counter efforts to abuse the change-of-address process.
4. To provide address information to the American Red Cross or other disaster relief organization about a customer who has been relocated because of disaster.
5. To support investigations related to law enforcement for fraudulent transactions.
6. To provide automatic updates to USPS customer systems using mail forwarding and change-of-address services.
7. To facilitate communication between USPS customers and the Postal Service with regard to change-of-address and address correction services.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. *Disclosure upon request.* The new address of a specific business or organization that has filed a permanent change-of-address order may be furnished to any individual on request. (Note: The new address of an individual or family will not be furnished pursuant to this routine use, unless authorized by one of the standard routine uses listed above or one of the specific routine uses listed below.) If a domestic violence shelter has filed a letter on official letterhead from a domestic violence coalition stating (i) that such domestic violence coalition meets the requirements of 42 U.S.C. § 10410 and (ii) that the organization filing the change of address is a domestic violence shelter, the new address shall not be released except pursuant to routine use d, e, or f pursuant to the order of a court of competent jurisdiction.

b. *Disclosure for Address Correction.* Disclosure of any customer's new permanent address may be made to a mailer, only if the mailer is in possession of the name and old address: from the National Change-of-Address Linkage (NCOALink®) file if the mailer is seeking corrected addresses for a mailing list; from the Computerized Forwarding System (CFS), from the Postal Automated Redirection System (PARS) if a mailpiece is undeliverable as addressed, or from the Locatable Address Conversion System if an address designation has been changed or assigned. Copies of change-of-address orders may not be furnished. In the event of a disaster or manmade hazard, temporary address changes may be disclosed to a mailer when, in the sole determination of the Postal Service, such disclosure serves the primary interest of the customer, for example, to enable a mailer to send medicines directly to the customer's temporary address, and only if the mailer is in possession of the customer's name and permanent address. If a domestic violence shelter has filed a letter on official letterhead from a domestic violence coalition stating (i) that such domestic violence coalition meets the requirements of 42 U.S.C. § 10410 and (ii) that the organization filing the change of address

is a domestic violence shelter, the new address shall not be released except pursuant to routine use d, e, or f pursuant to the order of a court of competent jurisdiction.

c. *Disclosure for Voter Registration.* Any customer's permanent change of address may be disclosed to a duly formed election board or registration commission using permanent voter registration. Copies of change of address orders may be furnished.

d. *Disclosure to Government Agency.* Any customer's permanent or temporary change of address information may be disclosed to a federal, state, or local government agency upon prior written certification that the information is required for the performance of its duties. A copy of the change of address order may be furnished. Name and address information may be disclosed to government planning authorities, or firms under contract with those authorities, if an address designation has been changed or assigned.

e. *Disclosure to Law Enforcement Agency.* Any customer's permanent or temporary change of address information may be disclosed to a law enforcement agency, for oral requests made through the Postal Inspection Service, but only after the Postal Inspection Service has confirmed that the information is needed for a criminal investigation. A copy of the change of address order may be furnished.

f. *Disclosure for Service of Process.* Any customer's permanent or temporary change of address information may be disclosed to a person empowered by law to serve legal process, or the attorney for a party in whose behalf service will be made, or a party who is acting pro se, upon receipt of written information that meets prescribed certification requirements. Disclosure will be limited to the address of the specifically identified individual (not other family members or individuals whose names may also appear on the change of address order). A copy of the change of address order may not be furnished.

g. *Disclosure for Jury Service.* Any customer's change of address information may be disclosed to a jury commission or other court official, such as a judge or court clerk, for purpose of jury service. A copy of the change of address order may be furnished.

h. *Disclosure at Customer's Request.* If the customer elects, change of address information may be disclosed to government agencies or other entities.

i. *Disclosure to a disaster relief organization.* Any customer's permanent or temporary change of address may be disclosed to the American Red Cross or other disaster relief organizations, if that address has been impacted by disaster or manmade hazard.

All routine uses are subject to the following exception: Information concerning an individual who has filed an appropriate protective court order with the postmaster/CFS manager will not be disclosed under any routine use except pursuant to the order of a court of competent jurisdiction.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Records generated from the source document are recorded on the Forwarding Control System file server and on tapes at CFS units. Electronic change-of-address records and related service records are also stored on disk and/or magnetic tape in a secured environment. Change-of-address records are consolidated in a national change-of-address (NCOA) file at the USPS IT Eagan Host Computing Services Center. Selected extracts of NCOA are provided in the secure data format represented by the NCOA^{Link} product to a limited number of firms under contract or license agreement with USPS.

Retrievability

Records are retrieved by the following methods:

For paper records: by name, address, date, and ZIP Code.

For electronic records: by name, address, date, ZIP Code™, and customer number for electronic change of address and related service records; by name, address, and email address for customer service records.

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.

Retention and Disposal

1. National change-of-address and mail forwarding records are retained 4 years from the effective date.
2. Delivery units access COA records from the Change-Of-Address Reporting System (COARS) database, which retains 2 years of information from the COA effective date. The physical change-of-address order is retained in the CFS unit for 30 days if it was scanned, or 18 months if it was manually entered into the national database.
3. Online user information may be retained for 12 months.

Records existing on paper are destroyed by shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

System Manager(s) and Address

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

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

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

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records should address inquiries to their local postmaster. Inquiries should contain full name, address, effective date of change order, route number (if known), and ZIP Code. Customers wanting to know if information about them is also maintained in the NCOA File should address such inquiries to: Manager, NCOA, National Customer Support Center, United States Postal Service, 6060 Primacy Parkway, Memphis, TN 38188.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers, personnel, contractors, service providers, and for call center operations, commercially available sources of names, addresses, and telephone numbers. For emergency change-of-addresses only, commercially available sources of names, previous addresses, and dates of birth. For alternative authentication, sources of names, previous and new addresses, dates of birth, and driver's state and license number.

USPS 800.050
System Name:
Address Matching for Mail Fraud Detection and Prevention.

System Classification

None.

System Location

USPS National Customer Support Center (NCSC) and USPS IT Eagan Host Computing Services Center.

System Manager(s)

Vice President, Product Innovation, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1010; (202) 268-6078.

Authority for Maintenance of the System

18 U.S.C. 1341, 1343, and 3061; 39 U.S.C. 401, 403, 404, 3003, and 3005.

Purpose(s)

1. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
2. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
3. To identify and mitigate potential fraud in the COA and Hold Mail processes.
4. To verify a customer's identity when applying for COA and Hold Mail services.
5. To facilitate mail fraud prevention for COA and Hold Mail services through address matching across USPS customer systems.
6. To facilitate the provision of accurate and reliable mail and package delivery services.

Categories of Individuals Covered by the System

Customers requesting COA mail forwarding or Hold Mail services.

Categories of Records in the System

1. *Customer information*: For COA requests, old and new address, email address(es), telephone numbers and device identification; for Hold Mail, address, email address(es), and telephone numbers.
2. *Online user information*: Device identification.

Record Source Categories

Individual customers requesting COA, mail forwarding, or Hold Mail services and other USPS customer systems.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses

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

Policies and Practices for Retrieval of Records

Retrieval is accomplished by a computer-based system, using one or more of the following elements: ZIP Code(s), address, telephone number, email address, device identification, and IP address.

Retention and Disposal

COA and Hold Mail records are retained in an electronic database for 10 years from the effective date.

Electronic records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

Administrative, Physical, and Technical Safeguards

Electronic records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced onsite 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 transmission is protected by encryption, dedicated lines, and authorized access codes.

Records Access Procedures

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

Contesting Records Procedures

See Notification Procedures below 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 in writing to the system manager. Inquiries must contain name, address, email, and other identifying information.

Exemptions Promulgated for the System

None.

History

None.

USPS 800.100
System Name:
Address Matching for Mail Processing.

System Location

Computer Operations Service Center; Engineering; Processing and Distribution Centers; and contractor site(s).

Categories of Individuals Covered by the System

USPS customers, including individual and business customers.

Categories of Records in the System

Names and mailing addresses of individuals and businesses.

Authority for Maintenance of the System

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

Purpose(s)

To improve the speed, accuracy, and certainty of mail delivery.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses

Standard routine uses 1. through 6. and 11. apply. In addition:

a. A mailpiece containing a barcode that is encoded with the address, but not name, of a customer derived from this system may be disclosed to a mailer if the Postal Service is unable to deliver the mailpiece, and returns it to the mailer as part of a requested return service.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, electronic and computer storage media, with names and addresses stored separately.

Retrievability

Retrieval is accomplished by a computer-based system, using one or more of the following elements: name, ZIP Code(s), street name, primary number, secondary number, delivery point, and/or carrier route identification.

Safeguards

The name and address database is obtained from a commercial vendor under strict contract and security controls. The database is maintained separately from USPS databases. Name data and address data within the commercial database are also stored separate from each other. In field deployment, name and address data are stored in an encrypted fashion. The database is not to be commingled with any agency records or databases, and is not to be used to update any agency record or database. No information is provided from the USPS into the commercial database or back to the vendor.

The database only operates on secure systems. Electronic transmissions of records are protected by encryption and access authorization codes. Records are kept on computers in controlled-access areas, with access limited to authorized personnel. Computers are protected by a cipher lock system, card key system, 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 use identifications, and file management. Contractors are subject to contract controls regarding security, as well as security compliance reviews.

Retention and Disposal

The database will be maintained until 90 days after termination of the contract or program, and then destroyed. During contract performance, the database is replaced by the vendor in its entirety no less frequently than every 90 days. To destroy the replaced version, the Postal Service employs sanitization procedures that ensure the complete destruction of information as specified by its information security policies.

System Manager(s) and Address

Vice President, Engineering Systems, United States Postal Service, 8403 Lee Highway, Merrifield, VA 22082.

Notification Procedure

Customers wanting to know if information about them is kept in this system of records must address inquiries in writing to the Manager, Letter Mail Technology, 8403 Lee Highway, Merrifield, VA 22082.

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above and the Postal Service Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Commercially available source of names and mailing addresses.

USPS 800.200
System Name:
Address Element Correction Enhanced Service (AECES).

System Location

USPS National Customer Support Center (NCSC).

Categories of Individuals Covered by the System

Customers whose corrected addresses are maintained to avoid repetitive correction by USPS personnel.

Categories of Records in the System

1. Customer information: name, incorrect address, and correct address.
2. Delivery information: reason mail cannot be delivered to an address.

Authority for Maintenance of the System

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

Purpose(s)

To provide address element correction services to increase the rate of properly addressed mail and improve delivery service to customers.

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. In addition:

a. Disclosure of a customer's corrected address or reason for nondelivery may be made to a mailer only if the mailer is in possession of the customer's address which contains a minor error.

All routine uses are subject to the following exception: A record concerning an individual who has filed an appropriate protective court order with the postmaster/CFS Manager will not be disclosed under any routine use except pursuant to the order of a court of competent jurisdiction.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases.

Retrievability

By name, correct or incorrect address, or by Secure Hash Algorithm 1 technique, which is a combination of name and incorrect address.

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.

Computer applications operate on a secure data communications network used exclusively by the Postal Service.

Secure hash algorithm 1 (SHA-1) encryption is used for the stored representation of an Update File of name and incorrect address records. The Update File is not commingled with any other agency records or databases.

Retention and Disposal

1. Records pending correction are retained no longer than 104 days.
2. Records in the Update File are retained 7 years from the last affirmative match.

Records existing on paper are disposed of or destroyed. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

System Manager(s) and Address

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

Vice President, Delivery and Post Office Operations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records should address inquiries to: Manager, National Customer Support Center, United States Postal Service, 6060 Primacy Parkway, Memphis, TN 38188. Inquiries should include full name, address, and ZIP Code. All known representations of incorrect name and/or address must be submitted in order to retrieve data to provide to the customer.

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above nd USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

USPS employees and mailers.

USPS 810.100 System Name: www.usps.com Registration.

System Location

Computer Operations Service Centers.

Categories of Individuals Covered by the System

Customers who register via the USPS Web site at *usps.com*.

Categories of Records in the System

1. *Customer information:* Name; customer ID(s); company name; job title and role; home, business, and billing address; phone number(s) and fax number; email(s); URL; text message number(s) and carrier; and Automated Clearing House (ACH) information.
2. *Identity verification information:* Question, answer, username, user ID, password, email address, text message address and carrier, and results of identity proofing validation.
3. *Business specific information:* Business type and location, business IDs, annual revenue, number of employees, industry, nonprofit rate status, mail owner, mail service provider, PC postage user, PC postage vendor, product usage information, annual and/or monthly shipping budget, payment method and information, planned use of product, age of website, and information submitted by, or collected from, business customers in connection with promotional marketing campaigns.
4. *Customer preferences:* Preferences to receive USPS marketing information, preferences to receive marketing information from USPS partners, preferred means of contact, preferred email language and format, preferred on-screen viewing language, product and/or service marketing preference.
5. *Customer feedback:* Method of referral to Web site.
6. *Registration information:* Date of registration.
7. *Online user information:* Internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of connection, Media Access Control (MAC) address, device identifier, information about the software acting on behalf of the user (i.e., user agent), and geographic location.

Authority for Maintenance of the System

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

Purpose(s)

1. To provide online registration with single sign-on services for customers.
2. To facilitate online registration, provide enrollment capability, and administer Internet-based services or features.
3. To maintain current and up-to-date address information to assure accurate and reliable delivery and fulfillment of postal products, services, and other material.
4. To obtain accurate contact information in order to deliver requested products, services, and other material.
5. To authenticate customer logon information for *usps.com*.
6. To permit customer feedback in order to improve *usps.com* or USPS products and services.
7. To enhance understanding and fulfillment of customer needs.
8. To verify a customer's identity when the customer establishes, or attempts to access his or her account.
9. To identify, prevent, and mitigate the effects of fraudulent transactions.
10. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
12. To identify and mitigate potential fraud in the COA and Hold Mail processes.
13. To verify a customer's identity when applying for COA and Hold Mail services. To provide online registration for Informed Address platform service for customers.
14. To authenticate customer logon information for Informed Address platform services.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By customer name, customer ID(s), phone number, mail, email address, IP address, text message address, and any customer information or online user information.

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.

For small business registration, computer storage tapes and disks are maintained in controlled-access areas or under general scrutiny of program personnel. Access is controlled by logon ID and password as authorized by the Marketing organization via secure Web site. Online data transmissions are protected by encryption.

Retention and Disposal

1. ACH records are retained up to 2 years.
2. Records stored in the registration database are retained until the customer cancels the profile record, 3 years after the customer last accesses records, or until the relationship ends.
3. For small business registration, records are retained 5 years after the relationship ends.
4. Online user information may be retained for 6 months.

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.

System Manager(s) and Address

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 810.200 System Name: www.usps.com Ordering, Payment, and Fulfillment.

System Location

Computer Operations Service Centers.

Categories of Individuals Covered by the System

Customers who place orders and/or make payment for USPS products and services through *usps.com*.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), phone and/or fax number, mail address, and email address.
2. *Payment information:* Credit and/or debit card number, type, and expiration date, billing information, ACH information.
3. *Shipping and transaction information:* Product and/or service ID numbers, descriptions, value, date, postage and fees, and prices; name and address(es) of recipients; order number and delivery status; electronic address lists; electronic documents or images; job number; and applicable citation or legend required by the foreign trade regulations.
4. Claims submitted for lost or damaged merchandise.
5. *Online user information:* Internet Protocol (IP) address, domain name, operating system version, browser version, date and time of connection, and geographic location.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, and 407; 13 U.S.C. 301–307; and 50 U.S.C. 1702

Purpose(s)

1. To fulfill orders for USPS products and services.
2. To promote increased use of the mail by providing electronic document preparation and mailing services for customers.
3. To provide shipping supplies and services, including return receipts and labels.
4. To provide recurring ordering and payment services for products and services.
5. To support investigations related to law enforcement for fraudulent financial transactions.
6. To satisfy reporting requirements for customs purposes.
7. To support the administration and enforcement of U.S. customs, export control, and export statistics laws.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. Customs declaration records may be disclosed to domestic and foreign customs agencies and postal operators, as well as intermediary companies involved in electronic data exchanges, for the purpose of facilitating carriage, security protocols, foreign or domestic customs processing, payment to operators, or delivery.

b. Records may be disclosed to the Office of Foreign Assets Control, the Bureau of Industry and Security, Customs and Border Protection, and other government authorities for the purpose of administering and enforcing export control laws, rules, and policies, including 50 U.S.C. 1702.

c. Customs declaration records may be disclosed to the U.S. Census Bureau for export statistical purposes pursuant to 13 U.S.C. 301-307.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By customer name, customer ID(s), phone number, mail or email address, or job number.

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 transmission is protected by encryption, dedicated lines, and authorized access codes. For shipping supplies, data is protected within a stand-alone system within a controlled-access facility.

Retention and Disposal

1. Records related to mailing online and online tracking and/or confirmation services supporting a customer order are retained for up to 30 days from completion of fulfillment of the order, unless retained longer by request of the customer.
2. Records related to shipping services and domestic and international labels are retained up to 90 days.

3. Delivery Confirmation and return receipt records are retained for 6 months.
4. Signature Confirmation records are retained for 1 year.
5. ACH records are retained for up to 2 years.
6. Customs declaration records stored in electronic data systems are retained 5 years, and then purged according to the requirement of domestic and foreign customs services. Other hard copy customs declaration records are retained 30 days.
7. Other records related to shipping services and domestic and international labels are retained up to 90 days.
8. Other customer records are retained for 3 years after the customer relationship ends.
9. Online user information may be retained for 12 months.

System Manager(s) and Address

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name, address, customer ID(s), and order number, if known.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 810.300 System Name: Offline Registration, Payment, and Fulfillment.

System Location

USPS Marketing Headquarters; Integrated Business Solutions Services Centers; Philatelic Fulfillment Service Center; area and district facilities; Post Offices; and contractor sites.

Categories of Individuals Covered by the System

Customers who register for USPS programs, place orders and/or make payment for USPS products and services via offline means.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), company name, job title, home, business, and billing address(es), phone number(s), fax number(s), e-mail, URL, verification question and answer, username, and password.
2. *Payment information:* Credit and/or debit card number, type, and expiration date; billing name and address; check; money order, ACH information.
3. *Shipping information:* Product and/or service ID number, name and address of recipient.
4. *Customer preferences:* Preferences to receive USPS marketing information, preferences to receive marketing information from USPS partners, preferred contact media, preferred e-mail format, product and/or service marketing preference.
5. *Customer feedback:* Method of referral.
6. *Order processing:* Inquiries on status of orders; claims submitted for defective merchandise; lists of individuals who have submitted bad checks.

Authority for Maintenance of the System

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

Purpose(s)

1. To provide offline registration services for customers.
2. To fulfill requests for USPS products, services, and other materials.
3. To authenticate customer information and permit customer feedback.
4. To operate recurring ordering and payment services for products and services.
5. To enhance understanding and fulfillment of customer needs.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage

Automated databases, computer storage media, and paper forms.

Retrievability

By customer name, customer ID(s), phone number, mail or e-mail address, or order number.

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 transmission is protected by encryption, dedicated lines, and authorized access codes. For shipping supplies, data is protected within a stand-alone system within a controlled-access facility.

Retention and Disposal

1. ACH records are retained up to 2 years.
2. Other records are retained up to 3 years after the customer relationship ends.

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.

System Manager(s) and Address

President and Chief Marketing/Sales Officer, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers and, for call center operations, commercially available sources of names, addresses, and telephone numbers.

USPS 820.100 System Name: Mailer Services — Applications and Approvals.

System Location

USPS Headquarters; Integrated Business Solutions Services Centers; National Customer Support Center (NCSC); district facilities; detached mailing units; and facilities that access USPS computers.

Categories of Individuals Covered by the System

Customers who apply for mail management and tracking products or services.

Categories of Records in the System

1. *Customer information:* Applicant and key contacts name, mail and e-mail address, phone number, fax number, customer ID(s), job title and/or role, employment status, company name, location, industry, monthly shipping budget, annual revenue, payment information, ACH information.
2. *Customer or product identification and authentication:* User and manager customer ID(s) and/or passwords; customer signature, date, last four digits of Social Security Number (SSN); USPS site; security personnel name, signature, date, telephone number, and last four digits of SSN; USPS location information; D-U-N-S Number; postage meter numbers; permit numbers; POSTNET code; mailer ID(s); publication name(s) and ID(s); and name(s) of authorized users.
3. *Mail practices and delivery information:* Type of mailing equipment and/or containers used, mail preparation information, drop shipment sites and codes, compatibility with mailing automation equipment, presort options and tests, frequency of mailings, mail volume, primary type of mailing, destination information, use of contracted mail services, names and addresses of contractors and advertisers, publication name(s) and ID(s), and appointment times.
4. *Technical information:* Hardware, software, and equipment names, types, versions, and specifications; media preferences; mail site specifications.
5. *Product usage and payment information:* Package volumes, package weights, product ordered, quantity ordered, billing information, products used, ordered date, inventory date, and usage measure dates.
6. *Customer feedback:* Method of referral.

Authority for Maintenance of the System

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

Purpose(s)

1. To provide application services for mail management and tracking products and services.
2. To authenticate applicant information, assign computer logon IDs, and qualify and assist users.
3. To provide product and/or service updates, service, and support.
4. To collect accurate technical data to ensure the proper operation of electronic data transmission and software.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By customer name, customer ID(s), or logon ID.

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.

Retention and Disposal

1. Logon records are retained 1 year after computer access.
2. ACH records are retained up to 2 years.
3. Security access records are retained 2 years after computer access privileges are cancelled.
4. Other customer records are retained 4 years after the customer relationship ends.

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.

System Manager(s) and Address

President and Chief Marketing/Sales Officer, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Mail Entry and Payment Technology, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries should contain name, customer ID(s), if any, and/or logon ID.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 820.200 System Name: Mail Management and Tracking Activity.

System Location

USPS Headquarters; Integrated Business Solutions Services Centers; USPS IT Eagan Host Computing Services Center; and Mail Transportation Equipment Service Centers.

Categories of Individuals Covered by the System

Customers who use USPS mail management and tracking services.

Categories of Records in the System

1. *Customer information:* Customer or contact name, mail and email address(es), title or role, phone number(s), text message number, and cell phone carrier.
2. *Identification information:* Customer ID(s), last four digits of Social Security Number (SSN), D-U-N-S Number; mailer and mailing ID, advertiser name/ID, username, and password.
3. *Data on mailings:* Paper and electronic data on mailings, including postage statement data (such as volume, class, rate, postage amount, date and time of delivery, mailpiece count), destination of mailing, delivery status, mailing problems, presort information, reply mailpiece information, container label numbers, package label, Special Services label, article number, and permit numbers.
4. *Payment information:* Credit and/or debit card number, type, and expiration date; ACH information.
5. *Customer preference data:* Hold mail begin and end date, redelivery date, delivery options, shipping and pickup preferences, drop ship codes, comments and instructions, mailing frequency, preferred delivery dates, and preferred means of contact.
6. *Product usage information:* Special Services label and article number.
7. *Mail images:* Images of mailpieces captured during normal mail processing operations.

Authority for Maintenance of the System

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

Purpose(s)

1. To provide mail acceptance, induction, and scheduling services.
2. To fulfill orders for mail transportation equipment.
3. To provide customers with information about the status of mailings within the USPS network or other carrier networks.
4. To provide customers with mail or package delivery options.
5. To provide business mailers with information about the status of mailings within the USPS mail processing network.
6. To help mailers identify performance issues regarding their mail.
7. To provide delivery units with information needed to fulfill requests for mail redelivery and hold mail service at the address and for the dates specified by the customer.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

By customer name, customer ID(s), logon ID, mailing address(es), 11-digit ZIP Code, or any Intelligent Mail barcode.

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.

Retention and Disposal

1. CONFIRM records are retained for up to 30 days.
2. Records related to ePubWatch, Confirmation Services and hold mail services are retained for up to 1 year.
3. Special Services and drop ship records are retained 2 years.
4. ACH records are retained up to 2 years.
5. Mailpiece images will be retained up to 3 days.
6. Other records are retained 4 years after the relationship ends.
7. USPS and other carrier network tracking records are retained for up to 30 days for mail and up to 90 days for packages and special services.

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.

System Manager(s) and Address

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries should contain name, customer ID(s), if any, and/or logon ID.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers and, for call center operations, commercially available sources of names, addresses, and telephone numbers.

USPS 820.300 System Name: Informed Delivery.

System Location

USPS Headquarters; Wilkes-Barre Solutions Center; and Eagan, MN.

Categories of Individuals Covered by the System

1. Customers who are enrolled in Informed Delivery notification service.
2. Mailers that use Informed Delivery notification service to enhance the value of the physical mail sent to customers.

Categories of Records in the System

1. *Customer information:* Name; customer ID(s); mailing (physical) address(es) and corresponding 11-digit delivery point ZIP Code; phone number(s); email address(es); text message number(s) and carrier.
2. *Customer account preferences:* Individual customer preferences related to email and online communication participation level for USPS and marketing information.
3. *Customer feedback:* Information submitted by customers related to Informed Delivery notification service or any other postal product or service.
4. *Subscription information:* Date of customer sign-up for services through an opt-in process; date customer opts-out of services; nature of service provided.
5. *Data on mailpieces:* Destination address of mailpiece; Intelligent Mail barcode (IMb); 11-digit delivery point ZIP Code; and delivery status; identification number assigned to equipment used to process mailpiece.
6. *Mail Images:* Electronic files containing images of mailpieces captured during normal mail processing operations.
7. *User Data associated with 11-digit ZIP Codes:* Information related to the user's interaction with Informed Delivery email messages, including but not limited to, email open and click-through rates, dates, times, and open rates appended to mailpiece images (user data is not associated with personally identifiable information).
8. *Data on Mailings:* Intelligent Mail barcode (IMb) and its components including the Mailer Identifier (Mailer ID or MID), Service Type Identifier (STID) and Serial Number.

Authority for Maintenance of the System

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

Purpose(s)

1. To support the Informed Delivery notification service which provides customers with electronic notification of physical mail that is intended for delivery at the customer's address.
2. To provide daily email communication to consumers with images of the letter-size mailpieces that they can expect to be delivered to their mailbox each day.
3. To provide an enhanced customer experience and convenience for mail delivery services by linking physical mail to electronic content.
4. To obtain and maintain current and up-to-date address and other contact information to assure accurate and reliable delivery and fulfillment of postal products, services, and other material.
5. To determine the outcomes of marketing or advertising campaigns and to guide policy and business decisions through the use of analytics.
6. To identify, prevent, or mitigate the effects of fraudulent transactions.
7. To demonstrate the value of Informed Delivery in enhancing the responsiveness to physical mail and to promote use of the mail by commercial mailers and other postal customers.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database and computer storage media.

Retrievability

By customer email address, 11-Digit ZIP Code and/or the Mailer ID component of the Intelligent Mail Barcode.

Safeguards

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. Access is controlled by logon ID and password. Online data transmissions are protected by encryption.

Retention and Disposal

1. Mailpiece images will be retained up to 7 days (mailpiece images are not associated with personally identifiable information). Records stored in the subscription database are retained until the customer cancels or opts out of the service.

2. User data is retained for 2 years, 11 months.
3. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice. Any records existing on paper will be destroyed by burning, pulping, or shredding.

System Manager(s) and Address

Vice President, Product Innovation, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260

Notification Procedure

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

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Individual customers who request Informed Delivery notification service; *usps.com* account holders; other USPS systems and applications including those that support online change of address, mail hold services, Premium Forwarding Service, or PO Boxes Online; commercial entities, including commercial mailers or other Postal Service business partners and third-party mailing list providers.

USPS 830.000 System Name: Customer Service and Correspondence.

System Location

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

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-ASK-USPS, other toll-free contact centers, or the Business Service Network (BSN), as well as customers with product-specific service or support issues.

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, D-U-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.

Authority for Maintenance of the System

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

Purpose(s)

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.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

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

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.

Retention and Disposal

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.

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.

System Manager(s) and Address

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

.

Notification Procedure

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.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers and, for call center operations, commercially available sources of names, addresses, and telephone numbers.

USPS 840.000 System Name: Customer Mailing and Delivery Instructions.

System Location

USPS Headquarters, Prohibitory Order Processing Center, districts, Integrated Business Solutions Services Centers, and Post Offices.

Categories of Individuals Covered by the System

1. Customers requesting delivery of mail through an agent and the agent to whom the mail is to be delivered.
2. Customers who are visually or physically disabled and unable to use or read conventionally printed materials and who are receiving postage-free matter in their delivery areas.
3. Customers whose mailboxes do not comply with USPS standards and regulations.
4. Customers who elect to have their names and addresses, or the name and address of their children under 19 years of age or a deceased spouse, placed on the list of individuals who do not want mailed to them sexually oriented advertisements (SOAs) or pandering advertisements.
5. Rural route customers.

Categories of Records in the System

1. *Customer information:* Name, address, phone number, customer ID(s), signature, application number, names and birth dates of children under 19; reports of mailbox irregularities and date; postmaster signature.
2. *Verification information:* Photocopies of IDs, customer name, address, signature, statement from competent authority as being visually or physically impaired from being able to use or read conventional reading matter.
3. *Agency information:* Agent name, address, signature, and phone number.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, 3008, 3010, and 3403.

Purpose(s)

1. To provide for efficient and secure mail delivery services.
2. To permit authorized delivery of mail to the addressee's agent.
3. To enable the efficient processing of mail for visually or physically disabled customers.
4. To protect customers from mail fraud and identity theft.
5. To maintain a list of addressees that do not want SOA material mailed to them, available for mailers to comply with statutory requirements; and to maintain records as necessary to provide protections requested by an addressee against individual mailers under the Pandering Advertisement statutes.
6. To assist rural carrier leave replacements who might be unfamiliar with assigned route and box numbers of rural route customers.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. Information may be disclosed for the purpose of identifying an address as an address of an agent to whom mail is delivered on behalf of other persons. This routine use does not authorize the disclosure of the identities of persons on behalf of whom agents receive mail.

All routine uses are subject to the following exception: Information concerning an individual who has filed an appropriate protective court order with the postmaster will not be disclosed under any of the general routine uses except pursuant to the order of a court of competent jurisdiction.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

By customer name, address, and application number, or by customer ID(s).

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.

Retention and Disposal

1. Records related to customer requests not to have mailed to them SOAs or pandering advertisements are retained up to 5 years after request.
2. Other records are retained 1 year from the date the customer relocates, cancels an order, corrects a cited mailbox irregularity, or terminates the special instruction.

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.

System Manager(s) and Address

For SOA and pandering advertisement prohibitory orders: Vice President, Pricing, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For other delivery records: Vice President, Delivery and Post Office Operations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system pertaining to mail delivery by agents, noncompliant mailboxes, with regard to free matter for the visually disabled, or pertaining to rural routes must address inquiries to their local postmasters. Customers should include name, address, and other identifying information.

Customers wanting to know if information about them is maintained in this system pertaining to requests not to have mailed to them SOAs and pandering advertisements must address inquiries to the system manager. Customers should include name, address, application number, and the date of filing, if applicable.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers; cosigners of the request for delivery of mail through an agent; medical personnel or other competent authorities; and USPS personnel.

USPS 850.000 System Name: Auction Files.

System Location

USPS Mail Recovery Center.

Categories of Individuals Covered by the System

Customers who participate in or request information about USPS auctions.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), mail and e-mail address, and phone number.
2. *Payment information:* Credit and/or debit card number, type, and expiration date; check; or money order.
3. *Customer feedback:* Means of referral.

Authority for Maintenance of the System

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

Purpose(s)

1. To maintain a list of names and addresses of customers participating in or requesting information about auctions.
2. To accurately process delivery and payment.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

By customer name, customer ID(s), or other identifier.

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.

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.

Retention and Disposal

Records are retained up to 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.

System Manager(s) and Address

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

Notification Procedure

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

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 860.000
System Name:
Financial Transactions.

System Location

USPS Headquarters; Integrated Business Solutions Services Centers; Accounting Service Centers; anti-money laundering support group; and contractor sites.

Categories of Individuals Covered by the System

1. Customers who use online payment or funds transfer services.
2. Customers who file claims or make inquiries related to online payment services, funds transfers, money orders, and stored-value cards.
3. Customers who purchase funds transfers or stored-value cards in an amount of $1000 or more per day, or money orders in an amount of $3000 or more per day, or who purchase or redeem any such services in a manner requiring collection of information as potential suspicious activities under anti-money laundering requirements. Recipients of funds transfers and the beneficiaries of funds from money orders totaling $10,000 in 1 day.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), mail and e-mail address, telephone number, occupation, type of business, and customer history.
2. *Identity verification information:* Date of birth, username and/or ID, password, Social Security Number (SSN) or tax ID number, and driver's license number (or other type of ID if driver's license is not available, such as Alien Registration Number, Passport Number, Military ID, Tax ID Number). (*Note:* For online payment services, SSNs are collected, but not retained, in order to verify ID.)
3. *Billers registered for online payment services:* Biller name and contact information, bill detail, and bill summaries.
4. *Transaction information:* Name, address, and phone number of purchaser, payee, and biller; amount, date, and location; credit and/or debit card number, type, and expiration; sales, refunds, and fees; type of service selected and status; sender and recipient bank account and routing number; bill detail and summaries; transaction number, serial number, and/or reference number or other identifying number, pay out agent name and address; type of payment, currency, and exchange rate; Post Office information such as location, phone number, and terminal; employee ID numbers, license number and state, and employee comments.
5. *Information to determine credit-worthiness:* Period at current residence, previous address, and period of time with same phone number.
6. *Information related to claims and inquiries:* Name, address, phone number, signature, SSN, location where product was purchased, date of issue, amount, serial number, and claim number.
7. *Online user information:* Internet Protocol (IP) address, domain name, operating system version, browser version, date and time of connection, and geographic location.

Authority for Maintenance of the System

39 U.S.C. 401, 403, and 404; 31 U.S.C. 5318, 5325, 5331, and 7701.

Purpose(s)

1. To provide financial products and services.
2. To respond to inquiries and claims related to financial products and services.
3. To fulfill requirements of anti-money laundering statutes and regulations.
4. To support investigations related to law enforcement for fraudulent financial transactions.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

Standard routine uses 1. through 7., 10., and 11. apply. Legally required disclosures to agencies for law enforcement purposes include disclosures of information relating to money orders, funds transfers, and stored--value cards as required by anti-money laundering statutes and regulations.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, microfiche, and paper.

Retrievability

For online payment and funds transfer services, information is retrieved by customer name, customer ID(s), transaction number, or address.

Claim information is retrieved by name of purchaser or payee, claim number, serial number, transaction number, check number, customer ID(s), or ZIP Code.

Information related to anti-money laundering is retrieved by customer name; SSN; alien registration, passport, or driver's license number; serial number; transaction number; ZIP Code; transaction date; data entry operator number; and employee comments.

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.

Retention and Disposal

1. Summary records, including bill due date, bill amount, biller information, biller representation of account number, and the various status indicators, are retained 2 years from the date of processing.
2. For funds transfers, transaction records are retained 3 years.
3. Records related to claims are retained up to 3 years from date of final action on the claim.
4. Forms related to fulfillment of anti-money laundering requirements are retained 5 years from the end of the calendar quarter in which they were created.
5. Related automated records are retained the same 5-year period and purged from the system quarterly after the date of creation.
6. Enrollment records related to online payment services are retained 7 years after the subscriber's account ceases to be active or the service is cancelled.
7. Account banking records, including payment history, Demand Deposit Account (DDA) number, and routing number, are retained 7 years from the date of processing.
8. Online user information may be retained for 6 months.

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.

System Manager(s) and Address

Chief Financial Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

For online payment services, funds transfers, and stored-value cards, individuals wanting to know if information about them is maintained in this system must address inquiries in writing to the Chief Marketing Officer. Inquiries must contain name, address, and other identifying information, as well as the transaction number for funds transfers.

For money order claims and anti-money laundering documentation, inquiries should be addressed to the Chief Financial Officer. Inquiries must include name, address, or other identifying information of the purchaser (such as driver's license, Alien Registration Number, Passport Number, etc.), and serial or transaction number. Information collected for anti-money laundering purposes will only be provided in accordance with Federal anti-money laundering laws and regulations.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers, recipients, financial institutions, and USPS employees.

Systems Exempted From Certain Provisions of the Act

USPS has established regulations at 39 CFR 266.9 that exempt information contained in this system of records from various provisions of the Privacy Act in order to conform to the prohibition in the Bank Secrecy Act, 31 U.S.C. 5318(g)(2), against notification of the individual that a suspicious transaction has been reported.

USPS 870.100
System Name:
Trust Funds and Transaction Records.

System Location

USPS Headquarters Marketing; Integrated Business Solutions Services Centers; district offices; Post Offices; and detached mailing units.

Categories of Individuals Covered by the System

Customers who are users of trust fund payment accounts.

Categories of Records in the System

1. *Customer information:* Customer and key contact name, mail and e-mail address, phone and fax number(s); D-U-N-S Number; customer ID(s), taxpayer ID number.
2. *Transactional information:* Permit authorizations and numbers, postage paid, postage class transaction dates, volume, weight, and revenue of mailing, postage indicium created, estimated annual postage, percent by mailing type, type of user, mailing data files including USPS location where the mail was entered.
3. *Information necessary for processing electronic payments:* Bank name, contact name, bank address and telephone number, bank account number, bank transit ABA number, voided check, credit and/or debit card number, type, and expiration date; ACH information.

Authority for Maintenance of the System

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

Purpose(s)

1. To establish and maintain trust fund accounts and process payments.
2. To ensure revenue protection.
3. To provide information and updates to users of these accounts.
4. To enhance understanding and fulfillment of customer needs.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated database, computer storage media, and paper.

Retrievability

By customer name or customer ID(s), account number, and/or address.

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.

Retention and Disposal

1. ACH records are retained up to 2 years.
2. Other records in this system are retained up to 4 years after the relationship ends.

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.

System Manager(s) and Address

President and Chief Marketing/Sales Officer, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

To access Permit records, customers must make a written request to their local postmaster. Correspondence must include name, address, account number, company name, mailing location, and a clear description of the issue.

To access all other records, customers must make a written request to the system manager. Correspondence must include name, address, account numbers, and other identifying information.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 870.200 System Name: Postage Validation Imprint (PVI), Electronic Verification System (eVS), Postage Meter, and PC Postage Customer Data and Transaction Records.

System Location

USPS Headquarters, USPS facilities, Integrated Business Solutions Services Centers, and partner locations.

Categories of Individuals Covered by the System

Postage evidencing system users.

Categories of Records in the System

1. Customer information: Contact name, address, and telephone number; registration identifiers; company name; and change of address information.
2. Identification information: Customer/system ID(s), IP address(es), date of device installation, device ID number, device model number, and certificate serial number.
3. Mailing and transaction information: Tracking ID, package identification code (PIC), customer-provided package/transaction attribute data, postage paid, contract pricing, package attribute data, USPS collection and source system identifiers, mailpiece images, and package destination and origin.

Authority for Maintenance of the System

39 U.S.C. 401, 403, and 404; 39 CFR Part 501.

Purpose(s)

1. To enable responsible administration of postage evidencing system activities.
2. To enhance understanding and fulfillment of customer needs.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. The name and address of an authorized user of a postage meter or PC Postage product (postage evidencing systems), printing a specified indicium will be furnished to any person provided the user is using the postage meter or PC Postage product for business purposes.

b. Customer-specific records and related sampling systems in this system may be disclosed to eVS customers, indicia providers, and PC Postage providers, including approved shippers, for revenue assurance to ensure accuracy of postage payment across payment systems, and to otherwise enable responsible administration of postage evidencing system activities.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

By customer name and by numeric file of postage evidencing systems ID number, or by customer ID(s).

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.

Retention and Disposal

1. ACH records are retained up to 2 years. Records of payment are retained up to 7 years.
2. Other records in this system are retained up to 7 years after a customer ceases using a postage evidencing system.
3. Within the Postal Service and directly to eVS customers, or through third-party software providers (including meter and PC Postage providers) for the purpose of enabling responsible administration of revenue assurance and other postage evidencing system activities, facilitating remediation of postage disparities, and meeting SOX compliance requirements, in accordance with 39 CFR Part 501.

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.

System Manager(s) and Address

Vice President, Mail Entry and Payment Technology, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Customers wanting to know if information about them is maintained in this system of records must address inquires in writing to: Manager, Payment Technology, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Inquiries should include the individual's name and customer ID.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers; authorized service providers of postage evidencing systems; and USPS personnel.

USPS 880.000 System Name: Post Office and Retail Services.

System Location

USPS Headquarters, Consumer and Industry Affairs; Integrated Business Solutions Services Centers; Accounting Service Centers; and USPS facilities, including Post Offices and contractor locations.

Categories of Individuals Covered by the System

1. Customers who apply for or purchase products and services at Post Offices, online, or at other retail sites. This includes products and services related to passports, Post Office boxes, caller services, and self-service equipment.
2. Senders and recipients of Extra Services.
3. Authorized users of Post Office boxes and caller services.
4. Customers with inquiries or claims relating to Extra Services.
5. Customers requesting delivery of mail to alternate locations.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), customer Personal Identification Numbers (PINs), company name, phone number, mail and e-mail address, text message number, record of payment, passport applications and a description of passport services rendered, and Post Office box and caller service numbers.
2. *Identity verification and biometric information:* Driver's license; two forms of ID; signature; photographic image via self-service equipment; fingerprints, date of birth, and Social Security Numbers (SSNs) as required for passports by the State Department.
3. *Recipient information:* Name, address, and signature.
4. Names and addresses of persons authorized to access a Post Office box or caller service.
5. *Claim and inquiry information:* Mailer and addressee name, mail and e-mail address, and phone number; claimant signature; claim or inquiry description, number, and status.
6. *Payment information:* Credit and/or debit card number, type, and expiration date.
7. *Product information:* Article number and class/services purchased.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, 407, and 411; 22 U.S.C. 214; 31 U.S.C. 7701

Purpose(s)

1. To enable customers to apply for and purchase nonfinancial products and services at Post Offices and other retail locations.
2. To provide customers with mail or package delivery options.
3. To ensure accurate and secure mail delivery.
4. To respond to inquiries and claims related to Extra Services.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. Disclosure of boxholder applicant name/address and the names of other persons listed as receiving mail on PS Form 1093, *Application for Post Office Box or Caller Service*, may be made to a federal, state, or local government agency upon prior written certification that the information is required for the performance of its duties. A copy of PS Form 1093 may be furnished.

b. Disclosure of boxholder applicant name/address may be made to a person empowered to serve legal process, or the attorney for a party in whose behalf service will be made, or a party who is acting pro se, on receipt of written information that meets prescribed certification requirements. A copy of PS Form 1093 will not be furnished.

c. Disclosure of boxholder applicant name/address and the names of other persons listed as receiving mail on PS Form 1093 may be made, on prior written certification from a foreign government agency citing the relevance of the information to an indication of a violation or potential violation of law and its responsibility for investigating or prosecuting such violation, and only if the address is (a) outside the United States and its territories, and (b) within the territorial boundaries of the requesting foreign government. A copy of PS Form 1093 may be furnished.

All routine uses are subject to the following exception: Information concerning an individual who has filed an appropriate protective court order with the postmaster will not be disclosed under any routine use except pursuant to the order of a court of competent jurisdiction.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By name, customer ID(s), phone number, mail or e-mail address, or transaction or article number.

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.

Retention and Disposal

1. Passport applications are mailed on the day of acceptance with fees and documentation. Records related to passports are retained 2 years.
2. Records related to Extra Services for domestic and international Express Mail items are retained up to 1 year.
3. Domestic and international Extra Services records are retained 2 years. Records relating to Post Office boxes and caller services are retained up to 2 years after the customer relationship ends.
4. Records collected via self-service equipment are retained up to 2 years.
5. Records related to credit and/or debit card transactions are retained 2 years.
6. Records related to inquiries and claims are retained 3 years from final action on the claim.
7. Records related to retail transactions are retained up to 5 years.

Records existing on paper are destroyed by shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

System Manager(s) and Address

Chief Marketing/Sales Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Delivery and Post Office Operations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Notification Procedure

For records relating to Post Office boxes, caller services, self-service, and passports, inquiries made in person must be made by the subject individual at the local Post Office. Requestors must identify themselves with a driver's license or military, government, or other form of acceptable identification.

Note: For passports, inquiries are best directed to the Department of State, which maintains the original case file.

For Extra Services, information can be obtained from the facility where the service was obtained, or can be accessed on *usps.com*. Inquiries should include name, date of mailing, and article number. For domestic or international Extra Services claims, customers can write a letter, including name, date of claim, and claim number, to Accounting Services, PO Box 80143 (for domestic claims) or PO Box 80146 (for international claims), St. Louis, MO, 63180, or call 866-974-2733. For international inquiries, customers can call 800-222-1811.

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 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

USPS 890.000 System Name: Sales, Marketing, Events, and Publications.

System Location

USPS Headquarters Marketing and Public Policy; Integrated Business Solutions Services Centers; National Customer Service Center; Area and District USPS facilities; Post Offices; and contractor sites.

Categories of Individuals Covered by the System

Customers who interact with USPS sales personnel, respond to direct marketing messages, request publications, respond to contests and surveys, and attend USPS events.

Categories of Records in the System

1. *Customer information:* Customer and key contacts' names, mail and e-mail addresses, phone, fax and pager numbers; job descriptions, titles, and roles; other names and e-mails provided by customers.
2. *Identifying information:* Customer ID(s), D-U-N-S Numbers, USPS account numbers, meter numbers, and signatures.
3. *Business specific information:* Firm name, size, and years in business; number of employees; sales and revenue information; business sites and locations; URLs; company age; industrial classification numbers; use of USPS and competitors products and services; types of customers served; customer equipment and services; advertising agency and spending; names of USPS employees serving the firm; and calls made.
4. *Information specific to companies that act as suppliers to USPS:* Contract start and end dates, contract award number, contract value, products and/or services sold under contract.
5. Information provided by customers as part of a survey or contest.
6. *Payment information:* Credit and/or debit card number, type, expiration date, and check information; and ACH information.
7. *Event information:* Name of event; role at event; itinerary; and membership in a PCC.
8. *Customer preferences:* Preferences for badge name and accommodations.

Authority for Maintenance of the System

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

Purpose(s)

1. To understand the needs of customers and improve USPS sales and marketing efforts.
2. To provide appropriate materials and publications to customers.
3. To conduct registration for USPS and related events.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

For sales, events, and publications, information is retrieved by customer name or customer ID(s), mail or e-mail address, and phone number.

For direct marketing, information is retrieved by Standard Industry Code (SIC) or North American Industry Classification System (NAISC) number, and company name.

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 transmission is protected by encryption.

Retention and Disposal

1. Records relating to organizations and publication mailing lists are retained until the customer ceases to participate.
2. ACH records are retained up to 2 years. Records relating to direct marketing, advertising, and promotions are retained 5 years.
3. Other records are retained 3 years after the relationship ends.

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.

System Manager(s) and Address

President and Chief Marketing/Sales Officer, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Consumer and Industry Affairs, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

For information pertaining to sales, inquiries should be addressed to: Office of Sales Performance Assessment, 475 L'Enfant Plaza SW, Washington, DC 20260.

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

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers, USPS personnel, and list providers.

USPS 900.000 System Name: International Services.

System Location

USPS Headquarters, Integrated Business Solutions Services Centers, and USPS facilities.

Categories of Individuals Covered by the System

Customers shipping to or from international locations.

Categories of Records in the System

1. *Customer information:* Customer name, customer ID(s), customer signature, date and place of birth, signed certification regarding sender or recipient identity, and contact information.
2. Name and address of senders and addressees.
3. *Information pertaining to mailings:* Information supplied through customs declaration forms: contents, product information, quantity, order number, volume, destination, weight, origin, value, price, Harmonized Commodity Description and Coding System (HS) Tariff number, product classification information, license or certificate number, Automated Export System (AES) internal transaction number or exemption, signature, date, postage and fees, insurance information, type of mailing, and applicable citation or legend required by the Foreign Trade Regulations.
4. Customs barcode scan data.
5. Company name; contact name, title, and phone and fax number; mail and email address; after-hours contact name and phone number; Tax ID number; Permit account number; and CAPS account number.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, and 407; 13 U.S.C. 301–307; and 50 U.S.C. 1702.

Purpose(s)

1. To provide international mailings and business services.
2. To provide USPS scan data to customers for mail tracking purposes.
3. To support customized mail agreements with international customers.
4. To support the administration and enforcement of U.S. customs, export control, and export statistics laws.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

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

a. Customs declaration records may be disclosed to domestic and foreign customs agencies and postal operators, as well as intermediary companies involved in electronic data exchanges, for the purpose of facilitating carriage, security protocols, foreign or domestic customs processing, payment to operators, or delivery.

b. Records may be disclosed to the Office of Foreign Assets Control, the Bureau of Industry and Security, Customs and Border Protection, and other government authorities for the purpose of administering and enforcing export control laws, rules, and policies, including 50 U.S.C. 1702.

c. Customs declaration records may be disclosed to the U.S. Census Bureau for export statistical purposes pursuant to 13 U.S.C. 301–307.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

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

Retrievability

By customer name(s) or address(es) (sender or recipient), ID number(s), and barcode tracking number(s).

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.

Retention and Disposal

1. Customs declaration records stored in electronic data systems are retained 5 years, and then purged according to the requirements of domestic and foreign customs services.
2. Other customs declaration records are retained 30 days.

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.

System Manager(s) and Address

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

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

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers and USPS personnel.

USPS 900.100 System Name: Customs Data Received from Foreign Posts.

System Location

USPS Headquarters, Integrated Business Solutions Services Centers, and USPS facilities.

Categories of Individuals Covered by the System

Customers shipping from international locations. Customers receiving items shipped from international locations.

Categories of Records in the System

1. The S10 13-character item identifier or any bilaterally agreed identifier.
2. The full name and postal address of the mailer.
3. The name and postal address of the intended recipient.
4. The gross weight of the item.
5. The total value of the item with the currency used.
6. The nature of the content (gift, document, a commercial sample, or some other content).
7. For each distinct type of content of the item: its description, the quantity and unit of measurement, its value, and its net weight.
8. For commercial items: the HS tariff number, the country of origin of the goods.
9. For items that require a Universal Postal Union (UPU) customs declaration form CN23: the importer's reference and details; the type and identifier of each document accompanying the item (invoice, certificate, license, authorization for goods subject to quarantine or other documents depending on the content and origin and destination of the item); other information and observations provided by the mailer and relevant for customs control, including, but not limited to, information about quarantine restrictions and the numbers of any licenses related to the item.

Authority for Maintenance of the System

39 U.S.C. 401, 404, and 407; Section 343(a) of the Trade Act of 2002, P.L. 107-210, and international agreements or regulations.

Purpose(s)

1. To collect data necessary for customs purposes.
2. To support processes related to the international exchange of mail.
3. To support operational purposes.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

Standard routine uses 1. through 7., 10., and 11. In addition:

Customs declaration records may be disclosed to domestic customs officials. When USPS has executed an agreement with a foreign postal operator for the exchange of customs declaration records, discretionary routine use disclosures for records exchanged in accordance with the agreement may be further restricted to the extent provided by the agreement.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System Storage

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

Retrievability

1. The S10 13-character item identifier or any bilaterally agreed identifier.
2. The full name and postal address of the mailer.
3. The name and postal address of the intended recipient.
4. The gross weight of the item.
5. The total value of the item with the currency used.
6. The nature of the content (gift, document, a commercial sample, or some other content).
7. For each distinct type of content of the item: its description, the quantity and unit of measurement, its value, and its net weight.
8. For commercial items: the HS tariff number, the country of origin of the goods.
9. For items that require a Universal Postal Union (UPU) customs declaration form CN23: the importer's reference and details; the type and identifier of each document accompanying the item (invoice, certificate, license, authorization for goods subject to quarantine or other documents depending on the content and origin and destination of the item); other information and observations provided by the mailer and relevant for customs control, including, but not limited to, information about quarantine restrictions and the numbers of any licenses related to the item.

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.

Retention and Disposal

Customs declaration records stored in electronic data systems are retained 5 years, and then purged according to the requirements of domestic and foreign customs services.

Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

System Manager(s) and Address

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

Notification Procedure

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

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers and USPS personnel.

USPS 910.000 System Name: Identity and Document Verification Services.

System Location

USPS Marketing, Headquarters; Integrated Business Solutions Services Centers; and contractor sites.

Categories of Individuals Covered by the System

1. Customers who apply for identity and document verification services.
2. Customers who may require identity verification for postal products and services.

Categories of Records in the System

1. *Customer information:* Name, address, customer ID(s), telephone number, text message number and carrier, mail and email address, date of birth, place of birth, company name, title, role, and employment status.
2. *Customer preference information*: Preferred means of contact.
3. Names and contact information of users who are authorized to have access to data.
4. *Verification and payment information:* Credit or debit card information or other account number, government issued ID type and number, verification question and answer, and payment confirmation code. ***Note:*** Social Security Number and credit or debit card information are collected, but not stored, in order to verify ID.
5. *Biometric information*: Fingerprint, photograph, height, weight, and iris scans. ***Note:*** Information may be collected, secured, and returned to customer or third parties at the request of the customer, but not stored.
6. *Digital certificate information:* Customer's public key(s), certificate serial numbers, distinguished name, effective dates of authorized certificates, certificate algorithm, date of revocation or expiration of certificate, and USPS-authorized digital signature.
7. *Online user information*: Device identification.
8. *Transaction information:* Clerk signature; transaction type, date and time, location, source of transaction; product use and inquiries; Change of Address (COA) and Hold Mail transactional data.
9. Electronic information related to encrypted or hashed documents.
10. *Recipient information:* Electronic signature ID, electronic signature image, electronic signature expiration date, and timestamp.

Authority for Maintenance of the System

39 U.S.C. 401, 403, 404, and 411.

Purpose(s)

1. To provide services related to identity and document verification services.
2. To issue and manage public key certificates, user registration, email addresses, and/or electronic postmarks.
3. To provide secure mailing services.
4. To protect business and personal communications.
5. To enhance personal identity and privacy protections.
6. To improve the customer experience and facilitate the provision of accurate and reliable delivery information.
7. To identify, prevent, or mitigate the effects of fraudulent transactions.
8. To support other Federal Government Agencies by providing authorized services.
9. To ensure the quality and integrity of records.
10. To enhance the customer experience by improving the security of COA and Hold Mail processes.
11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
12. To identify and mitigate potential fraud in the COA and Hold Mail processes.
13. To verify a customer's identity when applying for COA and Hold Mail services.
14. To provide an audit trail for COA and Hold Mail requests (linked to the identity of the submitter).
15. To enhance remote identity proofing with a Phone Validation and One-Time Passcode solution.

Routine Uses of Records 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 Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage

Automated databases, computer storage media, and paper.

Retrievability

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

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.

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

For authentication services and electronic postmark, electronic data is transmitted via secure socket layer (SSL) encryption to a secured data center. Computer media are stored within a secured, locked room within the facility. Access to the

database is limited to the system administrator, database administrator, and designated support personnel. Paper forms are stored within a secured area within locked cabinets.

Retention and Disposal

1. Records related to Pending Public Key Certificate Application Files are added as received to an electronic database, moved to the authorized certificate file when they are updated with the required data, and records not updated within 90 days from the date of receipt are destroyed.
2. Records related to the Public Key Certificate Directory are retained in an electronic database, are consistently updated, and records are destroyed as they are superseded or deleted.
3. Records related to the Authorized Public Key Certificate Master File are retained in an electronic database for the life of the authorized certificate.
4. When the certificate is revoked, it is moved to the certificate revocation file.
5. The Public Key Certificate Revocation List is cut off at the end of each calendar year and records are retained 30 years from the date of cutoff. Records may be retained longer with customer consent or request.
6. Other records in this system are retained 7 years, unless retained longer by request of the customer.
7. Records related to electronic signatures are retained in an electronic database for 3 years.
8. Other categories of records are retained for a period of up to 30 days.
9. Driver's License data will be retained for 5 years.
10. COA and Hold Mail transactional data will be retained for 5 years.

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.

System Manager(s) and Address

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1500.

Notification Procedure

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

Record Access Procedures

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

Contesting Record Procedures

See Notification Procedure and Record Access Procedures above.

Record Source Categories

Customers.

Tell Us Your Thoughts!

We hope that you found the *Guide to Privacy and the Freedom of Information Act* handbook to be helpful. Your comments will help us improve future editions. Please take a moment to fill out this survey and let us know what you think. Please mark your responses with an "X". Thanks!

Legend: **E**=Excellent **VG**=Very Good **G**=Good **F**=Fair **P**=Poor **NU**=Not Used

				E	VG	G	F	P
1.	Please indicate your reasons for using the handbook and how you would rate the handbook at providing you with the following information or other information you were seeking:							
	a.	To get general privacy information (e.g., sharing or disclosing information, or customer preferences)	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	b.	To get information about USPS *policies* regarding privacy	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	c.	To get information about USPS *procedures* regarding privacy (including the Privacy Act)	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	d.	To get general Freedom of Information Act (FOIA) information (e.g., how to make or process a FOIA request)	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	e.	To get information about FOIA procedures	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	f.	To get System of Records (SOR) Information	☐ Yes → ☐ No	☐	☐	☐	☐	☐
	g.	Other (specify) _____	☐ Yes → ☐ No	☐	☐	☐	☐	☐

			E	VG	G	F	P	NU
2.	What is your overall impression of the handbook?		☐	☐	☐	☐	☐	
3.	How would you rate the organization of the handbook?		☐	☐	☐	☐	☐	
4.	How would you rate the usefulness of the exhibits?		☐	☐	☐	☐	☐	☐
5.	How would you rate the handbook at providing the information you were seeking?		☐	☐	☐	☐	☐	
6.	Please rate the following sections:							
	a.	Introduction (pages 1-5)	☐	☐	☐	☐	☐	☐
	b.	Laws, Guidelines, and Policies (pages 7-26)	☐	☐	☐	☐	☐	☐
	c.	Privacy Procedures (pages 11-26)	☐	☐	☐	☐	☐	☐
	d.	Freedom of Information Act Procedures (pages 27-47)	☐	☐	☐	☐	☐	☐
	e.	System of Records (appendix)	☐	☐	☐	☐	☐	☐
7.	How would you rate USPS on its privacy protections?		☐	☐	☐	☐	☐	☐
8.	How would you rate your level of comfort in trusting the USPS not to share personal information?		☐	☐	☐	☐	☐	☐

9. Did you use this handbook as a USPS employee, USPS business customer, or USPS residential customer? (Mark all that apply)
☐ USPS Employee ☐ Business Customer ☐ Residential Customer

10. In your opinion, does the handbook contain:
☐ Too much information ☐ Just the right amount of information ☐ Not enough information

11. In your opinion, was the handbook:
☐ Easy to understand ☐ Somewhat easy to understand ☐ Difficult to understand

			Very Likely	Likely	Not Likely
12.	How likely are you to use this handbook again to answer any future questions about:				
		Privacy issues	☐	☐	☐
		FOIA information	☐	☐	☐
		USPS procedures	☐	☐	☐

13. We would appreciate your suggestions on how to improve this handbook.

Thank you!

For more information about USPS privacy policies, visit *www.usps.com*.

This page intentionally left blank