

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 6, 2014 as follows:

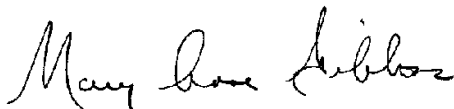
The chapter, subchapter, part, appendix, or section...	titled...	was...	in <i>Postal Bulletin</i> issue number...	with an issue date of....
Appendix – Privacy Act System of Records				
Section E	Complete Text of Systems of Records	revised to account for the collection of applicant ID numbers from applicants who file an inquiry or complaint.	22382	2-6-14

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

Handbook AS-353

February 2014
Transmittal Letter

- A. Introduction.** Key strategies of the Postal Service's Transformation Plan 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 original publication dated September 2005.
- 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 a completely revised appendix of Privacy Act systems of records, as last published in their entirety in the *Federal Register*. In addition, chapters 1 through 4 were revised to clarify current procedures. For ease of use, rules involving special categories of records, such as customer names and addresses, were relocated from chapter 4 to a new chapter 5.
- 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:
- MARY ANNE GIBBONS
GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT
US POSTAL SERVICE
475 L'ENFANT PLZ SW RM 6004
WASHINGTON DC 20260
PHONE: 202-268-2950
- F. Effective Date.** This handbook is effective February 2014.



Mary Anne Gibbons
General Counsel and Executive Vice President

Contents

1 Introduction	1
1-1 Purpose of This Handbook	1
1-2 Customer Trust and Privacy Protection	1
1-3 Handbook Application	1
1-4 Roles and Responsibilities	2
1-4.1 General Responsibility	2
1-4.2 Specific Responsibility	2
1-4.2.1 Officers, Managers, and Employees	2
1-4.2.2 Suppliers, Business Partners, and Customers	2
1-4.2.3 Chief FOIA Officer	2
1-4.2.4 Chief Privacy Officer	3
1-4.2.5 Manager, Records Office	3
1-4.2.6 Freedom of Information Act Requester Service Centers	3
1-4.2.7 Freedom of Information Act Public Liaison	4
1-4.2.8 Freedom of Information Act Coordinator	4
1-4.2.9 Records Custodian	5
1-4.2.10 Manager, Corporate Information Security Office	5
1-4.2.11 General Counsel	5
1-4.2.12 Chief Postal Inspector	5
1-4.2.13 Office of Inspector General	6
1-5 Definitions	6
1-5.1 Record	6
1-5.2 System of Records	6
1-5.3 Customers	6
1-5.4 Individual	6
1-5.5 Legal Hold Notice	7
1-5.6 Retention Period	7
2 Laws, Guidelines, and Policies	9
2-1 The Best of Public and Private Practices	9
2-2 Mail Protections	9
2-3 Federal Laws	9
2-3.1 Postal Reorganization Act	9
2-3.2 Privacy Act	9
2-3.3 Freedom of Information Act	10
2-3.4 E-Government Act of 2002	10
2-3.5 Gramm-Leach-Bliley Act	11

2-3.6 Children’s Online Privacy Protection Act	11
2-4 Federal Agency Guidelines	11
2-4.1 Federal Trade Commission Privacy Principles	11
2-4.2 Office of Management and Budget Privacy Guidelines	12
2-5 Postal Service Policies	12
2-5.1 Customer Privacy Policy	12
2-5.2 Marketing E-mail Policy	12
2-5.3 Supplier Policy	13
2-5.4 Monitoring of Postal Service Equipment.	13
3 Privacy Procedures	15
3-1 General	15
3-2 Collecting Information from Customers, Employees, or Other Individuals.	15
3-2.1 Collection	15
3-2.2 Privacy Notice	15
3-2.3 Customer Choice	16
3-3 Managing Information Relating to Customers, Employees, or Other Individuals.	17
3-3.1 General	17
3-3.2 Managing a System of Records	17
3-3.3 Creating, Amending, or Deleting a System of Records	18
3-3.4 Privacy Impact Assessment and Security	19
3-4 Requests by Customers, Employees, or Other Individuals for Information About Themselves	19
3-4.1 Requests to Access Information	19
3-4.2 Requests to Amend Information	23
3-4.3 Appeals and Customer Redress	25
3-4.4 Fees.	25
3-5 Disclosing Customer, Employee, or Other Individuals’ Information to Third Parties	25
3-5.1 General	25
3-5.2 Internal Disclosures.	26
3-5.3 External Disclosures	26
3-5.4 Validating Records and Noting Disputes	26
3-5.5 Accounting of Disclosures	26
3-6 Operating a Customer Web Site.	28
3-7 Sending Marketing E-mail	28
3-8 Entering Into a Contract or Business Agreement	28
3-9 Computer Matching Programs	29
4 Freedom of Information Act Procedures	31
4-1 General	31
4-2 How to Make a Freedom of Information Act Request	31
4-2.1 Format and Content	31
4-2.2 Requests for Expedited Processing	32

Contents

4-2.3 Requests for Fee Waivers	32
4-2.4 Where to Direct Freedom of Information Act Requests	32
4-3 How to Process a Freedom of Information Act Request	33
4-3.1 General	35
4-3.2 Requests That Are Insufficient, Misdirected, or for Records That Do Not Exist.	35
4-3.3 Searches	35
4-3.4 Releasing Records	35
4-3.5 Withholding Records.	36
4-3.6 Appeal Rights	36
4-3.7 Time Limits	36
4-3.8 Retention	37
4-4 Records Available to the Public	37
4-4.1 Reading Rooms.	37
4-4.2 Business Change of Address	38
4-4.3 Permit Holder Data	38
4-4.4 Postage Evidencing System User Data	38
4-5 Records Which May Be Withheld From Disclosure	38
4-5.1 Exemption 1 (5 USC 552(b)(1)) — National Defense and Foreign Relations.	39
4-5.2 Exemption 2 (5 USC 552(b)(2)) — Personnel Rules and Practices	39
4-5.3 Exemption 3 (5 USC 552(b)(3)) — Federal Law.	39
4-5.4 Exemption 4 (5 USC 552(b)(4)) — Trade Secrets and Privileged Information.	40
4-5.5 Exemption 5 (5 USC 552(b)(5)) — Internal or Interagency Information.	40
4-5.6 Exemption 6 (5 USC 552(b)(6)) — Personal Information	40
4-5.7 Exemption 7 (5 USC 552(b)(7)) — Law Enforcement Records	41
4-5.8 Exemption 8 (5 USC 552 (b)(8)) — Financial Institutions.	41
4-5.9 Exemption 9 (5 USC 552 (b)(9)) — Geological Information	41
4-6 Fees	42
4-6.1 General	42
4-6.2 Aggregate Requests	42
4-6.3 Fee Waivers.	42
4-6.4 Requester Categories	42
4-6.5 How to Assess Fees	43
4-6.6 Advance Notice and Payment.	44
4-6.7 Accounting for Fees	45
4-7 Appeals.	45
4-7.1 General	45
4-7.2 Time Limit	45
4-7.3 Required Appeal Elements	45
4-7.4 Final Decision	46
4-8 Reporting	46
4-8.1 General	46
4-8.2 Submissions	47
4-8.3 FOIA Annual Report	47

5	Requests for Special Categories of Records	49
5-1	General	49
5-2	Requests for Employee or Customer Information	49
5-3	Congressional Requests	59
5-4	Records Subject to Litigation	59
6	Records Management	61
6-1	Records Management Policy	61
6-1.1	General	61
6-1.2	What You Need to Know About Records	61
6-1.3	Records Safeguards	62
6-2	Records Creation and Designation Guidelines	62
6-2.1	General	62
6-2.2	Creating a Record	62
6-2.3	Record Designation	62
6-2.4	Micrographics	63
6-2.4.1	Microform	63
6-2.4.2	Policy	63
6-2.4.3	Legal	64
6-2.4.4	Archival	64
6-2.4.5	Maintenance and Disposal	64
6-3	Retention	64
6-3.1	General	64
6-3.2	Record Series and Record Control Schedules	64
6-3.3	Retention Periods	64
6-4	Storage and Retrieval	65
6-4.1	General	65
6-4.2	Local Storage	65
6-4.3	National Archives and Records Administration and Federal Records Centers	65
6-4.4	Vital Records	66
6-5	Disposal	67
6-5.1	General	67
6-5.2	Disposal Methods	68
6-5.3	Disposal Procedures	69
6-6	Separation Procedure (Employee or Non-Employee Available)	69
6-6.1	General	69
6-6.2	Separation Procedures	69
6-7	Records Subject to Litigation and Legal Holds	70
6-7.1	General	70
6-7.2	Procedures to Follow to Issue a Legal Hold Notice	70
6-7.3	Procedures to Follow When a Legal Hold Notice Is Issued	71

Contents

Appendix – Privacy Act Systems of Records	73
Survey – Tell Us Your Thoughts!.....	155

This page intentionally left blank

Exhibits

Exhibit 3-2.2	
Procedures to Provide a Privacy Notice	16
Exhibit 3-2.3	
Procedures to Provide Choice	17
Exhibit 3-5.5	
Suggested Format for Memo on Disclosure	28
Exhibit 4-3	
FOIA Processing Checklist for Custodians	34
Exhibit 4-5	
Exemption 3 Statutes	39
Exhibit 5-2a	
Address Disclosure Chart	54
Exhibit 5-2b	
Change of Address or Boxholder Request Format — Process Servers	57
Exhibit 5-2c	
Address Information Request Format — Government Agencies	58
Exhibit 6-5.1	
Suggested Format for Records Disposal Notice.	68

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 Privacy Procedures

3-1 General

This chapter incorporates all privacy requirements including Privacy Act and privacy policies, described in chapter 2. The chapter is organized by activities that trigger privacy requirements and describes procedures that must be followed.

3-2 Collecting Information from Customers, Employees, or Other Individuals

3-2.1 Collection

The Postal Service may only collect and maintain information relating to customers, employees, or other individuals that is needed or relevant to carry out a purpose authorized by statute or by executive order. To the greatest extent practical, information should be collected directly from the customer, employee, or individual. The Postal Service may not collect or maintain information describing how individuals exercise their rights protected by the First Amendment, unless the Postmaster General determines that the information is necessary to carry out a statutory purpose of the Postal Service.

3-2.2 Privacy Notice

The following describes privacy notice requirements.

- a. *General.* When the Postal Service asks customers, employees, or other individuals to provide information about themselves and that information is maintained in a system of records, the Postal Service must provide an appropriate privacy notice. The Privacy Office must approve all new forms (hard copy and electronic) that collect customer, employee, or other individuals' information. This includes hard copy and electronic forms, new forms, and forms scheduled for revision and reprinting.
- b. *Content.* The privacy notice must contain the following information:
 - (1) For individual consumers, employees, or other individuals, the privacy notice must explain:
 - (a) The reason the information is being collected.

- (b) Whether providing it is mandatory or voluntary, and the effects of not providing it.
 - (c) The disclosures (known as routine uses) that may be made of the information.
 - (d) Which statute or executive order authorizes the collection.
 - (e) That the customer privacy policy is available on *usps.com*.
- (2) For business customers, the notice is a statement that the customer privacy policy is available on *usps.com*.
- c. *How to Provide Privacy Notice.* [Exhibit 3-2.2](#), Procedures to Provide a Privacy Notice, describes how to provide a privacy notice, if required under section [3-2.2a](#), at different points where information is collected from customers, employees, or other individuals.

Exhibit 3-2.2

Procedures to Provide a Privacy Notice

Contact Point	Postal Service Procedures to Provide a Privacy Notice
In Person (Retail, interviews, etc.)	<ul style="list-style-type: none"> ■ Content of the notice must meet requirements of section 3-2.2b. ■ Provide the notice in writing or orally. If oral, provide the notice before collecting data, and include a note with the maintained information that notice was provided orally.
Hard Copy Forms	<ul style="list-style-type: none"> ■ Content of the notice must meet requirements of section 3-2.2b. ■ Place the notice on the form near where data is collected, or provide a separate privacy notice before collecting the data (e.g., Notice 70).
Telephone	<ul style="list-style-type: none"> ■ Provide callers with a notice that meets the content requirements of section 3-2.2b via an automation system or orally. If automated, the system must deliver a statement, when the caller is transferred to an option where information may be collected and maintained in a system of records, that the Postal Service has a privacy policy, and allow the caller to access the full content of the notice on the menu of options. Alternatively, call center agents may provide oral notice of the policy in accordance with in-person procedures in this table. ■ If a caller requests additional information, the call center agent should mail the caller a privacy notice, or direct the caller, if a customer, to the <i>usps.com</i> privacy policy.
Online	<ul style="list-style-type: none"> ■ For employees, a privacy notice that meets the content requirement of section 3-2.2b must be available on the screen near where data is collected. ■ For customers, provide a link to the privacy policy on every page on <i>usps.com</i>.
E-mail	<ul style="list-style-type: none"> ■ If data may be collected as a result of an e-mail interaction and placed in a system of records, provide a privacy notice meeting the content requirements of section 3-2.2b. ■ Place the notice in the same e-mail that solicits data, or include the notice in the response to e-mails from the customer, employee, or other individual. ■ For information on marketing e-mail policy, see MI AS-350-2004-4.

3-2.3 **Customer Choice**

When customers provide their information when they register for or request a product or service and the Postal Service maintains the information in a system of records, the customers must be given a choice if the information may be used subsequently for a secondary use. Secondary uses include marketing a different product to the customer or sharing the information externally with third parties (other than Postal Service business partners or suppliers). Follow these procedures only if the Postal Service may want to contact the customer in the future for a secondary use.

- a. *Choice for Consumers requires “Opt-in.”* Opt-in choice requires an affirmative expression by the consumer that authorizes any secondary use.
- b. *Choice for Business Customers requires “Opt-out.”* Opt-out choice requires that the customer take an affirmative step to prevent any secondary use.
- c. *Customers must be able to freely modify their choice.* Customers must have the ability to modify their previous decision so that their current choice is incorporated.

[Exhibit 3-2.3](#), Procedures to Provide Choice, provides procedures on how to provide choice at different points where information is collected from a customer.

Exhibit 3-2.3
Procedures to Provide Choice

Contact Point	Postal Service Procedures to Provide Choice
In Person/Telephone	<ul style="list-style-type: none"> ■ Employees may direct the customer to <i>usps.com</i> to create a profile and select choice; may direct the customer to the Privacy Office at the address in section 1-4.2.3; or may provide the customer a privacy brochure that provides information about choice.
Hard-Copy Forms	<ul style="list-style-type: none"> ■ Provide text and opportunity to express choice for secondary uses on consumer forms.
Online	<ul style="list-style-type: none"> ■ Provide customers who register on <i>usps.com</i> with the ability to create a profile and select and amend their choices.
E-mail	<ul style="list-style-type: none"> ■ If a customer wants to establish or amend their preference, direct the customer to register, create, or edit a profile on <i>usps.com</i>. ■ For information on marketing e-mail policy, see MI AS-350-2004-4.

3-3 Managing Information Relating to Customers, Employees, or Other Individuals

3-3.1 General

The following describes procedures that must be followed if information about a customer, employee, or individual is maintained in a system of records. A system of records is a file, database, or program from which information about customers, employees, or individuals is retrieved by name or other identifier. These procedures must be followed whether the information is obtained directly from the customer, employee, or individual, or from some other source.

3-3.2 Managing a System of Records

Manage each system of records as follows:

- a. *Authorized System of Records.* If a manager or employee maintains information about a customer, employee, or individual in a system of records, that system of records must be authorized. A description of authorized systems of records is listed in the [Appendix](#).

- b. *Data Management Requirements.* The applicable system of records in the [Appendix](#) describes how information within the system must be managed. Specific data management requirements for each system of records include:
- (1) Locations where records covered by the system are maintained.
 - (2) Types of customers, employees, or individuals whose records are contained in the system.
 - (3) Types of records contained in the system.
 - (4) Legal authority for maintaining the system.
 - (5) Purpose(s) for which the system is maintained.
 - (6) Permissible routine uses (disclosures) of records within the system.
 - (7) Procedures for record storage, retrieval, safeguards, retention and disposal.
 - (8) Contact information for the system manager.
 - (9) Procedures for customers, employees, or individuals to access and request amendment of records.

3-3.3 **Creating, Amending, or Deleting a System of Records**

Create, amend, or delete a system of records as follows:

- a. *General.* Employees or managers must notify the Records Office if they are maintaining information about customers, employees, or other individuals in a system of records that is not authorized. The Records Office manages the process for creating, amending, or deleting an authorized system of records. The Records Office must accomplish the following steps before a program or system can be implemented or amended:
- (1) Draft a notice creating or amending a system of records.
 - (2) Send the notice to the CPO and relevant Postal Service departments for review and approval.
 - (3) Forward the notice to Congress and the OMB.
 - (4) Publish the notice in the *Federal Register*.
- b. *Criteria for Amending a System.* The manager(s) of a system must notify the Records Office if he or she is planning to make changes to a program or system which requires the authorized system of records to be amended. The following are examples of such changes:
- (1) Changing the types of individuals or the scope of the population on whom the records are maintained.
 - (2) Expanding the types of information maintained.
 - (3) Altering the purpose for which information is collected.
 - (4) Altering the manner in which the records are stored or retrieved so as to change the nature or scope of these records (an example is a change from a manual to an automated system).

- (5) Changing or adding a routine use (disclosures from the system).
- c. *Deleting a System.* When a need for maintaining records in a system of records no longer exists, the system manager must consult with the Records Office about deleting the system of records.

3-3.4 **Privacy Impact Assessment and Security**

Comply with Privacy Impact Assessment and security requirements as follows:

- a. *Privacy Impact Assessment (PIA).* The Privacy Office, in partnership with Information Security, conducts PIAs for personal information contained in IT systems as part of the Business Impact Assessment (BIA) process. The BIA is a document that addresses privacy and information security requirements of a new or existing information resource. It is the first phase of the Information Security Assurance (ISA) process, which protects information contained in the resource through its lifecycle. Regarding privacy, the BIA ensures privacy compliance and also determines the sensitivity of the system, which contributes to establishing the security plan for the resource. The executive sponsor of the information resource is responsible for completing and adhering to the BIA. Completed BIAs must be submitted to the CPO and the manager of the Corporate Information Security Office. Information about the BIA and template is available at <http://about.usps.com/who-we-are/privacy-policy/privacy-impact-assessments.htm>.
- b. *Security.* Information about customers, employees, or other individuals must be kept secure, in accordance with Handbook AS-805, *Information Security*.
- c. *Testing.* The use of customer, employee, or other individuals' information for testing purposes must meet all written approval requirements found in Handbook AS-805, *Information Security*. Requirements for approval apply regardless of where the testing is conducted.

3-4 Requests by Customers, Employees, or Other Individuals for Information About Themselves

Customers, employees, or individuals may request and obtain information about themselves that the Postal Service maintains in a system of records in accordance with this section.

3-4.1 **Requests to Access Information**

The following procedures govern customer, employee, or individual requests about whether the Postal Service maintains information about them and requests to access that information, as well as Postal Service responses to such requests.

- a. *How to Request Information.* Customers, employees, or other individuals should follow these procedures to request information about themselves.
- (1) *General.* Customers, employees, or other individuals who want to know whether the Postal Service maintains information about them in a system of records and obtain access to that information, should follow the procedures described in the applicable system of records. The procedures for each system of records are listed in the [Appendix](#). A records custodian may require appropriate identification and, when deemed appropriate, request that individuals provide either a notarized statement or a statement signed under penalty of perjury stating that they are the person they claim to be.
 - (2) *Where to direct the request.* Direct the request to the records custodian, if known, or to the manager of the Records Office, at the address in section [1-4.2.5](#). Direct requests for records maintained by the Postal Inspection Service or the Office of Inspector General to the addresses in sections [1-4.2.12](#) and [1-4.2.13](#). Employee requests to review or copy a record should be made to the installation where the record is kept. Employees requesting retired official personnel folders (OPFs) may direct the request to any office and specify the installation where review is desired. Headquarters employees should direct requests to:

CORPORATE PERSONNEL MANAGEMENT
475 L'ENFANT PLAZA SW, ROOM 1831
WASHINGTON, DC 20260
 - (3) *Content of request.* The requester should clearly mark the request "Privacy Act Request" and:
 - (a) Specify the information sought and include other information as required by the applicable system of records (in [Appendix](#)).
 - (b) Specify the system of records by name or number, as shown in the [Appendix](#), or otherwise reasonably identify the system of records.
 - (c) Provide enough information to identify the requester and to identify and locate the record.
 - (d) Include any other relevant information, such as preferences as to where and how to receive the information.
 - (4) *Customers registered on usps.com.* Customers that are registered users on *usps.com* may access their personal profile by logging into their account with their user name and password.
- b. *Responding to Requests:*
- (1) *Determine Sufficiency of Request.* Before disclosing any records, including whether records exist, the custodian should review the sufficiency of the request. Oral requests for records that are available to the public under section [4-4](#) may be answered by telephone. All other requests must be made in person or in

writing and follow the procedures in section [3-4.1a](#). The custodian must seek clarification from the requester if the information supplied to locate and identify the record is insufficient. Misdirected requests must be forwarded to the appropriate location with a copy of the referral to the requester.

- (2) *Respond to the Requester.* Custodians must acknowledge requests for records within 10 days (excluding weekends and federal holidays) of receipt. Custodians should date stamp the request upon receipt. If requested records are not immediately available, the custodian must give the requester a date of availability. If records cannot be found or have been destroyed, the custodian must inform the requester.
- (3) *Provide Records.* Once records are located, provide them to the requester as soon as practical, unless they should be withheld under section [3-4.1b\(6\)](#). The custodian must provide releasable records to the requester in writing or in person as follows:
 - (a) *In writing:* Send the requested information or copies of records to the requester via Certified Mail™, return receipt service requested, as soon as any required fees or statement of release are received.
 - (b) *In person:* Notify the requester when and where records will be available for inspection or copying, and comply with the requester's instructions if feasible. When a requester reviews records in person, the custodian or designee must be present and observe the requester's handling of the records. The custodian or designee must do the following:
 - Verify the requester's identity by checking official credentials such as a driver's license or similar identification.
 - Allow the requester to copy the record manually or with a copying machine.
 - Collect the records and any fees incurred.
 - Have the requester sign a statement that he or she reviewed the records.
- (4) *Additional instructions for response to employee requests.* Records are usually available for inspection and copying during regular business hours at the installation where the records are kept. The custodian may, however, designate other reasonable locations and times for inspection and copying of some or all of the records. Employees who want to review or copy their own records must do so on their own time, except as provided for under collective bargaining agreements.

Forward requests for a retired OPF to the installation indicated by the requester, or as determined by the custodian to the nearest postal facility. The custodian at the installation where the review is to take place must determine if the information is releasable under section [3-4.1b\(6\)](#). If releasable, the custodian can obtain

the OPF by sending an SF 127, *Request for Official Personnel Folder*, to:

NATIONAL PERSONNEL RECORDS CENTER
CIVILIAN PERSONNEL RECORDS
111 WINNEBAGO STREET
ST. LOUIS, MO 63118

When the custodian receives the OPF, the custodian must notify the requester that the information is available for review. After the requester reviews the OPF and there is a need for further review, the custodian may keep the files at the designated facility for a maximum of 30 days. If there is no further need to retain the files, the custodian must return the OPF by Registered Mail™ to the National Personnel Records Center.

- (5) *Additional Instructions for response to customer requests.* Customers must be given access to their information maintained by the Postal Service, except for confidential business data created by the Postal Service or derived from third parties, or if exempt under section [3-4.1b\(6\)](#).
- (6) *Denying Requests.* The Postal Service may only deny customer, employee, or individual requests to know whether the Postal Service maintains records about them, and/or to obtain access to those records, if the requester does not follow procedures in section [3-4.1](#), or if the information is exempt under section [3-4.1b\(7\)](#). The custodian must consult with appropriate counsel before denying a request. Denials must be in writing and signed by the custodian or designee. The document must state the reasons for the denial and advise the requester of the right to appeal to the general counsel. See section [3-4.3](#).
- (7) *Exceptions to Release of Information.* The following information may not be released in response to customer, employee, or other individual requests for information about themselves.
 - (a) *Confidential Sources.* Information that identifies an individual who has requested and has been expressly promised anonymity in providing information to the Postal Service. This exception applies only to Postal Inspection Service records (which may be disclosed only on the authority of the chief postal inspector); preemployment investigation records; recruiting, examining, training, and placement records; equal employment opportunity discrimination complaint investigations and counseling records; and postmaster selection records.
 - (b) *Civil Actions.* Records compiled in reasonable anticipation of a civil action or proceeding such as a lawsuit or administrative hearing.
 - (c) *Law Enforcement.* Records of disclosures of information to law enforcement agencies.
 - (d) *Testing Material.* Information within records that might compromise testing or examination materials.

- (e) *Registers*. Registers for positions to be filled. (On written request, an individual may be told whether prospects for appointment are good, fair, or unfavorable.)
 - (f) *Medical Records*. Medical or psychological records (including those received from the Department of Veterans Affairs, Public Health Service, or Office of Workers' Compensation Programs) when the medical officer determines that disclosure could have an adverse effect on the subject individual. These records may be made available to a physician designated in writing by the individual. In such cases, an accounting of disclosure must be filed. See section [3-5.5](#); also see 39 CFR 266.6(b)(4).
 - (g) *Uncirculated Supervisors' Notes*. Information about individuals in the form of uncirculated personal notes kept by Postal Service personnel, such as employees, supervisors, counselors, or investigators, which are not circulated to other persons. If notes are circulated, they become official records in a system of records and must be shown on request to the employee to whom they pertain. Official evaluations, appraisals, or estimates of potential must be made available to the employee to whom they pertain.
 - (h) *National Agency Checks*. Results of national agency checks and written inquiry investigations (NACI) conducted by the Office of Personnel Management. Advise individuals requesting NACI records to send their requests to:
OPM FEDERAL INVESTIGATIONS PROCESSING CENTER
PO BOX 618
BOYERS, PA 16018
 - (i) *Exempt Systems of Records*. Information contained in any system of records that is exempt from disclosure as allowed by the Privacy Act. Exempt systems of records are listed in the [Appendix](#).
- (8) *Recording Responses*. For requests from individuals, the custodian must complete PS Form 8170, *Freedom of Information Act and Privacy Act Request Report*, in accordance with section [4-8](#). The custodian must also keep an accounting of the disclosure in accordance with section [3-5.5](#).

3-4.2 **Requests to Amend Information**

This section covers procedures by which customers, employees, or other individuals may request an amendment of information about themselves that the Postal Service maintains in a system of records, and how the Postal Service responds to these requests.

- a. *How to Submit a Request*. Customers, employees, or other individuals should submit a request as follows:

- (1) *Oral Requests.* Oral requests can be made if the change concerns an error or correction that is unlikely to be disputed (for example, correcting a misspelling, misprint, mistake in computation, or other obvious error). The custodian may have the record changed without formally notifying the requester of the change. If the request may result in a dispute, the custodian must require that the request be made in writing.
 - (2) *Written Requests.* Except as stated above, all requests must be in writing. The request must be submitted to the custodian in accordance with the procedures described in the applicable system of records in the [Appendix](#). Requesters must clearly identify themselves, the record in question, and the change desired. Requesters must state the reasons for the change, which may be relevance, accuracy, timeliness, or completeness.
 - (3) *Customers registered on usps.com.* Customers that are registered users on *usps.com* may amend their personal profile by logging into their account with their user name and password.
- b. *How to Respond to a Request.* Custodians must follow these procedures to respond to a request:
- (1) *Acknowledge the request.* Within 10 days (excluding weekends and federal holidays) of any written request to amend a record, the custodian must acknowledge the request in writing and ask the requester for any additional information necessary for action on the request.
 - (2) *Act on the request.* Within 30 days (excluding weekends and federal holidays), the custodian must do the following:
 - (a) *Inquire.* Obtain more information as needed to determine whether amendment is appropriate.
 - (b) *Amend the information as necessary.* Correct or eliminate any information found incomplete, inaccurate, untimely, or irrelevant to the purpose of the system of records.
 - (c) *Notify the requester about the revised record.* Advise the requester of the change, and supply a courtesy copy of the revised record where practical. The custodian must also send a revised record to any person or agency to whom an accounting of disclosure has been made under section [3-5.5](#).
 - (d) *Denial.* 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 filed with the disputed record or may appeal the decision. See section [3-4.3](#).

3-4.3 **Appeals and Customer Redress**

The following procedures apply to appeals by customers, employees, or other individuals, as well as customer questions and inquiries regarding Postal Service customer privacy policies.

- a. *Appeals.* Customers, employees, or other individuals may appeal denials of their request as to whether the Postal Service maintains records about them, or to access or amend those records. Appeals must be in writing and directed to the general counsel within 30 days of the date of denial, or within 90 days from a request if the appeal concerns a failure of the custodian to make a determination. The general counsel may consider late appeals. The letter of appeal must include:
 - (1) Reasonable identification of the record the requester wishes to access or amend.
 - (2) A statement of the action appealed and relief sought.
 - (3) Copies of the request, the notification of denial, and any other related correspondence.

The general counsel should make a final decision within 30 days (excluding weekends and federal holidays) of the date of receipt of the appeal.

- b. *Customer Redress.* Customers who have questions or inquiries about Postal Service customer privacy policies, or treatment of their data under the policies, should direct questions to their local Postal Service contact, the program manager, or the Privacy Office at the address in section [1-4.2.4](#). Postal Service employees should contact the Privacy Office if they are unable to satisfy or answer the customer's inquiry.

3-4.4 **Fees**

Customers, employees, or other individuals may access, review, or amend their information free of charge. No fee is charged for the first copy of the requested record, up to the first 100 pages. The cost for additional or duplicate copies is \$0.15 per page. Deposit fees in Account Identifier Code (AIC) 127. The Postal Service does not charge for requests if fees do not exceed \$10.

3-5 **Disclosing Customer, Employee, or Other Individuals' Information to Third Parties**

3-5.1 **General**

Information about a customer, employee, or other individual contained in a system of records cannot be released to another person, including a spouse, except as allowed under this section.

3-5.2 **Internal Disclosures**

Information may be disclosed to any Postal Service employee, or employee of a supplier managing a Postal Service system of records, who needs the information in the performance of Postal Service duties.

3-5.3 **External Disclosures**

Information can only be disclosed externally under one of the following four conditions:

- a. *Consent.* The customer, employee, or individual has authorized the disclosure in writing. The requester must have a signed statement of consent from the customer, employee, or individual, dated no earlier than 1 year before the date the Postal Service receives the request. Customers, employees, or other individuals may invite third parties to be present when reviewing records, if they submit a written statement authorizing disclosure in their presence.
- b. *Statute.* The disclosure fits within one of 12 categories listed in the Privacy Act. See the [Appendix](#).
- c. *Routine Use.* The agency has established a routine use authorizing the disclosure. Routine uses for systems of records are contained in the [Appendix](#). To determine the complete list of routine uses that apply to a particular system of records, check the general list of routine uses that apply to the system, as well as the particular system itself to see if it contains any special routine uses.
- d. *Information that is Publicly Available.* Certain information relating to employees may be released. See section [5-2\(b\)](#). For information relating to the public, such as business change of address, permit holders, and other information, see section [4-4](#).

3-5.4 **Validating Records and Noting Disputes**

Before disclosing a record to a third party, the custodian must make reasonable efforts to ensure that it is accurate and complete enough to ensure fairness if a decision were made on the basis of the record. For example, it may be appropriate to advise recipients that the information was accurate as of a certain date. The custodian must clearly note any part of the record that is disputed and provide copies of any statement disputing the record.

3-5.5 **Accounting of Disclosures**

- a. *Requirement.* Custodians must keep an accurate accounting of every disclosure of information about an individual covered by a system of records, even if the disclosure is made at the individual's request. The only exceptions are as follows:
 - (1) Publicly available information. See section [4-4](#).
 - (2) Information disclosed to Postal Service employees or contractors in the performance of their Postal Service duties.
 - (3) Information disclosed to the individual to whom the information pertains.

- b. *Request for Accounting of Disclosures.* Individuals may request that the Postal Service provide its accounting of disclosures of records relating to themselves. The request must be made to the facility where the record is kept, and must clearly identify the requester and the system of records. Requests for accountings of disclosures pursuant to a computer match must be addressed to the Records Office manager at the address in section [1-4.2.5](#).
- c. *Response.* The custodian must notify the requester within 30 days (excluding weekends and federal holidays) of receipt of the request whether a record of disclosures exists. If such a record exists, the custodian must give the requester the disclosure information unless an exception under section [3-4.1b\(6\)](#) applies.
- d. *Disclosure Formats.* There are four formats for an accounting of disclosures:
 - (1) *General Format Guidance.* The format of an accounting of a disclosure is usually a memorandum to the file (see suggested format in [Exhibit 3-5.5](#)), a copy of the correspondence transmitting the disclosed information, a log, or other listing, and must show:
 - (a) The date, nature (such as employee accident record folder review), and purpose (such as legal proceeding) of the disclosure.
 - (b) The name and address of the agency or person to whom the disclosure was made.
 - (2) *Official Personnel Folders.* Use PS Form 6100-B, *OPF Disclosure Accounting Form*, to account for disclosure of information in OPFs to law enforcement officials. Use PS Form 6100-A, *OPF Disclosure Accounting Form*, to account for all other disclosures. For OPFs converted to electronic Official Personnel Folder (eOPF), a system-generated accounting of disclosure may be used in lieu of PS Form 6100-A or PS Form 6100-B.
 - (3) *Union Representatives.* Except for disclosures of OPF information, use PS Form 6105, *Disclosure of Information About Employees to Collective Bargaining Agents*, to account for disclosures to collective bargaining agents.
 - (4) *Inspection Service.* Use PS Form 2099, *Inspection Service Disclosure Record*, to document disclosure of investigative information about individuals.
- e. *Filing and Retention.* The disclosure form must be filed, cross-indexed, or otherwise associated with the disclosed record, so that a complete accounting of disclosures can be constructed. The accounting must be kept for 5 years or the life of the disclosed record, whichever is longer.

Exhibit 3-5.5

Suggested Format for Memo on Disclosure

<p>Record of Disclosure from System of Records in Compliance with 5 U.S.C. 552a(c)</p> <p>Pertaining to: _____ [name of individual] _____ Date: _____</p> <p>Information disclosed: _____ [state, summarize, or otherwise identify] _____</p> <p>Source: _____ [no. and name of system of records, identification of document(s), etc.] _____</p> <p>To: _____ [individual, organization (if any), and address] _____</p> <p>Purpose:</p> <p>Authority for disclosure: _____ [section of Act; no. of routine use; identification of written request or consent] _____</p>

3-6 Operating a Customer Web Site

Web sites 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 Web site provides links to external Web sites, follow the procedures in MI AS-610-2007-4, *Web Site Affiliation Program*.

3-7 Sending Marketing E-mail

The Postal Service's 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 that markets a different product or service than the customer may already receive from the Postal Service. Managers or employees intending to send a marketing e-mail must follow the procedures for notice and choice in [Exhibit 3-2.2](#) and [Exhibit 3-2.3](#). Complete procedures are available in MI AS-350-2004-4, *Marketing E-mail*.

3-8 Entering Into a Contract or Business Agreement

Suppliers and business partners with access to information relating to customers, employees, or individuals, or that help to build or operate a Web site or conduct a marketing e-mail campaign, must adhere to Postal Service privacy policies. Contracts and agreements, whether or not covered by Postal Service purchasing regulations, must include privacy clause(s). For procedures to ensure the appropriate clause is included, reference the

purchasing regulations at 39 CFR Part 601, purchasing guidelines at <http://about.usps.com/manuals/pm/welcome.htm>, and Privacy Clause 1-1. Consult the Privacy Office, Supply Management, or appropriate counsel as needed.

3-9 Computer Matching Programs

A computer matching program is any computerized comparison of a Postal Service automated system of records with an automated system of another agency or an internal system. When using computer matching programs, the Postal Service must comply with Privacy Act requirements. The Postal Service Data Integrity Board is responsible for the review and approval of all Postal Service computer matching activities. The records office manages the process. All proposals, whether from Postal Service organizations or other government agencies, must be submitted to the Records Office at the address in section [1-4.2.5](#). Submit proposals at least 3 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*.

This page intentionally left blank

4 Freedom of Information Act Procedures

4-1 General

The FOIA provides the public with access to records maintained by the Postal Service, unless the records are exempt from disclosure. It is also Postal Service policy to make its records available to the public to the maximum extent consistent with the public interest. This chapter includes procedures that implement FOIA and Postal Service policy.

4-2 How to Make a Freedom of Information Act Request

4-2.1 **Format and Content**

A FOIA request must be in writing, be a request for records, and bear the caption “Freedom of Information Act Request.” Other requests for information are considered informal requests, and should still be processed in accordance with this handbook.

A requester should include the following information in a FOIA request:

- a. The requester’s name, mailing address, and daytime telephone number.
- b. A reasonable description of the records sufficient to permit the custodian to locate them with a reasonable amount of effort, and a description of any desired formats to receive the records.
- c. If seeking information about a company, the exact name and address of the company (many companies use similar names).
- d. The maximum amount of fees the requester is willing to pay without prior notice. If no amount is stated, the requester is deemed willing to pay fees up to \$25.
- e. The requester is not required to provide reasons for the request. However, because some or all of the requested records may be exempt from disclosure, the requester may state any reason(s) he or she believes the record should be disclosed.

If necessary, the custodian may ask the requester for more information.

4-2.2 **Requests for Expedited Processing**

The requester may ask for expedited processing if able to demonstrate a compelling need. See section [4-3.7b](#).

4-2.3 **Requests for Fee Waivers**

The requester may ask that fees or the advance payment of fees be waived in whole or in part. See sections [4-6.3](#) and [4-6.6](#).

The waiver request must describe all of the following:

- How the information will be used.
- To whom it will be provided, including the public.
- How the public is to benefit from the disclosure.
- Any personal or commercial benefit that the requester expects from disclosure.
- The intended user's identity, qualifications, and expertise in the subject area.

4-2.4 **Where to Direct Freedom of Information Act Requests**

Requesters must direct FOIA requests to the appropriate FOIA Requester Service Center (RSC) as follows:

- a. *U.S. Postal Service Headquarters Records, Supply Management or Facilities Records, and Employee Listings.* USPS headquarters structure is separate from the rest of the organization; however, certain positions in the field report to headquarters functions. To see how the Postal Service is structured, visit <http://about.usps.com/who-we-are/leadership/welcome.htm>. FOIA requests for U.S. Postal Service Headquarters controlled records; Supply Management or Facilities controlled records including contracts, building leases, and other real estate transactions; or employee listings must be directed to:

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

Online: <https://pfoiapal.usps.com/palMain.aspx>

If requesters are unclear what office maintains the records they are seeking, the request should be submitted to the Manager Records Office. Personnel in the Records Office will then forward requests to the appropriate office(s).

- b. *U.S. Postal Service Field Records.* FOIA requests for U.S. Postal Service records controlled by area offices, district offices, Post Offices, or other field operations facilities must be directed to:

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

Online: <https://pfoiapal.usps.com/palMain.aspx>

- c. *Inspection Service Records.* FOIA requests for Inspection Service records must be directed to:
OFFICE OF COUNSEL
US POSTAL INSPECTION SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON, DC 20260
Telephone: 202-268-4538
- d. *Inspector General Records.* FOIA requests for Inspector General records must be directed to:
OFFICE OF INSPECTOR GENERAL
US POSTAL SERVICE
1735 N LYNN ST STE 10000
ARLINGTON, VA 22209
Fax: 703-248-4626
email: foia@uspsig.gov
Online: https://www.uspsig.gov/foia_request.htm

4-3 How to Process a Freedom of Information Act Request

Records custodians must process FOIA requests in accordance with the following procedures. A checklist of these steps is provided as [Exhibit 4-3](#).

Exhibit 4-3

FOIA Processing Checklist for Custodians

1. *Read the request carefully.* If the request is so vague or overly broad that you are unable to understand what records are being sought, ask the requester to give a “reasonable description” (see section [4-2.1](#)). A request does not necessarily fail the “reasonable description” requirement just because it is burdensome
2. *Process the request in a timely manner.* The law requires that FOIA requests be responded to within 20 working days from the date that the records custodian receives the request (see section [4-3.7a](#)). An extension is permitted only in unusual circumstances (see section [4-3.7c](#)).
3. *Determine fees.* Categorize the requester for purpose of assessing fees. Fees may be assessed for search, review, and duplication, depending on the category of the requester (see section [4-6.4](#)). Then determine if the requester has agreed to accept liability for costs and if advance notice or advance payment is required (see section [4-6.6](#)).
4. *Locate records.* Locate all responsive records, including those in storage. Search for records in electronic form or format, except when doing so would significantly interfere with the operation of the system.
5. *Release nonexempt records.* The general rule is that a record (or parts of a record) must be released unless it falls under an exemption (see section [4-5](#)). If parts of a record are released, the redacted (edited out) parts of the record should be bracketed with the cited exemption(s) written in the adjacent margin (see section [4-3.5](#)). Provide records in the format specified by the requester if readily reproduced in that format. For example, if the records can be made available in paper or on computer media and the requester asks to receive it on computer media, you must honor the requester’s preference (see section [4-3.4](#)).
6. *Write response letter.* All requests must be responded to in writing. If records are denied, the response letter must include the following elements: (a) a statement of the reason for the denial; (b) a citation to the exemption(s) applied (from section [4-5](#)); (c) a brief explanation of how the exemption applies to the withheld material; (d) if entire records or pages are withheld, a reasonable estimate of the number of records or pages, unless that information is exempt; and (e) a statement that the requester may appeal the denial (see section [4-7](#)).
7. *Complete PS Form 8170, Freedom of Information Act and Privacy Act Request Report.* If your organization processes a request received directly from the requester, you must complete PS Form 8170 and send it to the office indicated in section [4-8.2](#). If the Records Office refers a request to you, a PS Form 8170 will be included with the referral. Return this form, along with a copy of the response, to the Records Office after processing the FOIA request.
8. *Retain records.* Retain FOIA correspondence and record of all documents provided or denied for a period of 6 years from the end of the fiscal year in which the final response occurs.

4-3.1 **General**

The custodian or designee is responsible for locating requested records and determining whether to disclose them or to deny the request. The custodian or designee should consult as needed with the FOIA coordinator, the Records Office manager, or appropriate counsel before releasing or withholding records. The custodian or designee shall respond courteously and appropriately.

4-3.2 **Requests That Are Insufficient, Misdirected, or for Records That Do Not Exist**

If a custodian cannot locate a record based on the information furnished, the custodian must do the following:

- a. For insufficient requests, allow the requester to submit more information to describe the record. If feasible, the custodian should confer with the requester to clarify the request.
- b. Employees should forward misdirected requests to the appropriate FOIA RSC and notify the requester that the request has been forwarded.
- c. If there are no responsive records, notify the requester. Custodians are not required to create records in order to respond to requests.

4-3.3 **Searches**

The custodian must make reasonable efforts to locate the requested records, including those records in storage and in electronic format, except when such effort would significantly interfere with the operation of the information system. Custodians should maintain adequate documentation of their steps in conducting a search, including an accounting of search time, in order to properly calculate fees or respond to appeals. The cut-off date for records to be included as responsive to a FOIA request is the date the search for records begins. Custodians may extend the cut-off date at their discretion. There is no requirement under the FOIA to make automatic releases of records as they are created.

4-3.4 **Releasing Records**

The custodian must locate and provide nonexempt records within the required time limits in section [4-3.7](#). If records are provided by written response, the custodian must explain any fees charged and how they may be paid, attach copies of the requested records (in the format requested if feasible), and describe the reasons for any withholdings and appeal rights. As an alternative, the custodian may notify the requester in writing where and when records are available for copying. The custodian or a designee must be present during copying and collect any required fees. The custodian must send a letter to the requester confirming that records were so provided.

4-3.5 **Withholding Records**

The custodian must determine whether some or all of the documents or portions of the documents are exempt from disclosure and provide a response within the time limits required in section [4-3.7](#). The decision to withhold information must be in writing, signed by the custodian or designee, and must:

- a. Explain any fees to be charged and how they may be paid.
- b. Identify and explain all FOIA exemption(s) relied upon.
- c. Advise of appeal rights. See section [4-3.6](#).

The denial letter must include all nonexempt material, including any reasonable part of an exempt record that can be segregated, and a description of withholdings as follows. If records are withheld in part, black out or redact the exempt material and note the applicable exemption in the margin of the record. If entire records or pages are withheld, provide a reasonable estimate of the number of records or pages, unless such estimate would harm an interest protected by the exemption relied upon.

4-3.6 **Appeal Rights**

- a. Letters denying FOIA requests must include language such as the following:
“You have the right to appeal this response by writing to the General Counsel, United States Postal Service, 475 L’Enfant Plaza SW, Room 6004, Washington DC 20260, within 30 days of the date of this letter. The letter of appeal should include a statement about the action or failure to act being appealed, the reasons why it is believed to be erroneous, and the relief sought, along with copies of your original request, this letter, and any other related correspondence.”
- b. Letters denying requests for Inspector General records should use the same language as above but indicate that the appeal should be made to the address in section [1-4.2.13](#).

4-3.7 **Time Limits**

The custodian must respond to the requester in writing within the following time frames.

- a. *General*. The FOIA requires that requests be responded to within 20 days (excluding weekends and federal holidays). The 20-day period starts when the appropriate records custodian receives a request, and the request describes or has been clarified to describe records in a manner allowing them to be identified and located with a reasonable amount of effort. 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.
- b. *Expedited Processing*. Requests for expedited processing must be granted when a requester demonstrates a compelling need. Compelling need exists if:
 - (1) Failure of the requester to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

- (2) In the case of a request made by a person primarily engaged in disseminating information, there is an urgency to inform the public concerning actual or alleged federal government activity. Within 10 calendar days of receipt of the request for expedited processing, the custodian must notify the requester in writing whether the request is granted. If granted, the custodian must process the request for records as soon as practical. If denied, the custodian must include appeal rights in the letter under section [4-3.6](#).
- c. *Unusual Circumstances.* The custodian may extend the response period under unusual circumstances. Unusual circumstances include requests requiring: (1) review of voluminous records; (2) a search of facilities other than the one processing the request; or (3) consultation with another agency, or two or more components of the Postal Service, having a substantial interest in the records. Within the initial 20-day response period, the custodian must send a letter to the requester stating the reason for the delay. If the response can be made within 10 additional working days from the end of the response period, the letter should include the expected response date. Otherwise the letter should provide the requester an opportunity to limit the scope of the request and/or arrange an alternative time frame for response. If the requester and the custodian cannot agree on scope or time frames, then the custodian must process the FOIA request as soon as reasonably possible, and send a letter to the requester confirming the lack of agreement and providing an estimated response date. The custodian must send a copy of all correspondence to the manager of the Records Office.

4-3.8 **Retention**

The custodian must retain FOIA correspondence and a record of all documents provided or denied for a period of 6 years from the end of the fiscal year in which the final response occurs.

4-4 Records Available to the Public

The following information is considered public information, and can be released to the public.

4-4.1 **Reading Rooms**

Information maintained in public and electronic reading rooms.

- a. *Public Reading Room.* The Postal Service maintains a public reading room in the Postal Service library. The following material is available:
 - (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 the Postal Operations Manual (POM) 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 bid protest decisions.
 - (5) Postal Service manuals and publications that affect members of the public.
- b. *Electronic Reading Room.* The FOIA electronic reading room indexes information routinely available to the public, including material contained in the public reading room, as well as records previously released under FOIA that have been the subject of multiple requests. The electronic reading room may be accessed at <http://about.usps.com/who-we-are/foia/readroom/welcome.htm>. The Office of Inspector General reading room may be accessed at http://www.uspsoig.gov/reading_room.cfm.

4-4.2 **Business Change of Address**

The new address of any business that has filed a change of address notice.

4-4.3 **Permit Holder Data**

The name and address of the holder of a particular bulk mail permit, permit imprint, or similar permit, and the name of any individual applying for a permit on behalf of a holder. Lists of permit holders may not be disclosed.

4-4.4 **Postage Evidencing System User Data**

The name and address of a user of a postage evidencing system (postage meter or PC Postage) may be disclosed provided the system is used for a business purpose. As evidence of business purpose, the request must include the original or copy of the envelope or wrapper on which the indicium is printed and a copy or description of the contents. Lists of users of postage evidencing systems may not be disclosed. All requests must be sent to:

POSTAGE TECHNOLOGY MANAGEMENT
 US POSTAL SERVICE
 475 L'ENFANT PLZ SW RM 4200 NB
 WASHINGTON DC 20260

4-5 **Records Which May Be Withheld From Disclosure**

The FOIA (5 USC 552(b)(1–9)) provides nine exemptions under which records or portions of records may be withheld from public disclosure. A custodian may disclose exempt information as a matter of discretion if that disclosure is not prohibited by law and would not cause any foreseeable harm. The nine exemptions and records covered under each are listed in sections [4-5.1](#) through [4-5.9](#).

4-5.1 **Exemption 1 (5 USC 552(b)(1)) – National Defense and Foreign Relations**

Exemption 1 applies to classified national defense and foreign relations information.

4-5.2 **Exemption 2 (5 USC 552(b)(2)) – Personnel Rules and Practices**

Exemption 2 applies to records related solely to internal personnel rules and practices that are either (a) too trivial to be of genuine public interest, or (b) would enable circumvention of laws or regulations.

4-5.3 **Exemption 3 (5 USC 552(b)(3)) – Federal Law**

Exemption 3 applies to information that is exempt from disclosure under another federal statute. Examples include the Postal Reorganization Act and 39 U.S.C. 410(c) and 412. The table below 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.

Exhibit 4-5

Exemption 3 Statutes

Exempting Statute	Type of Information Covered
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. Examples: <ul style="list-style-type: none"> ■ Information about methods of handling valuable Registered Mail. ■ Money order records. ■ Technical information on postage meters and prototypes submitted for approval before leasing to mailers. ■ Market surveys. ■ Records indicating rural carrier lines of travel. ■ 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. ■ Records that would be of potential benefit to firms in economic competition with the Postal Service. ■ Information that could materially increase procurement costs. ■ Information that might compromise testing or examination materials.
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 or 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.

Exempting Statute	Type of Information Covered
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.
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 or for any purpose.
18 U.S.C. 1461	Records concerning nonmailable matter.
18 U.S.C. 2510-2520	Records relating to wiretap requests and information.
Federal Rules of Criminal Procedure- Rule 6(e)	Grand jury information.
Inspector General Act of 1978, Section 7(b)	Confidentiality of employee complaint information

4-5.4 **Exemption 4 (5 USC 552(b)(4)) – Trade Secrets and Privileged Information**

Exemption 4 applies to trade secrets and privileged or confidential commercial or financial information provided to the Postal Service by a party outside the Postal Service, such as a supplier or customer. The custodian must follow the procedures in section [5-2c](#) before releasing third-party business information.

4-5.5 **Exemption 5 (5 USC 552(b)(5)) – Internal or Interagency Information**

Exemption 5 applies to 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 deliberative process privilege, attorney-client privilege, and attorney work-product privilege. The deliberative process privilege permits withholding of predecisional, 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.

4-5.6 **Exemption 6 (5 USC 552(b)(6)) – Personal Information**

Exemption 6 applies to personal information, including medical and personnel files, the disclosure of which would be a clearly unwarranted invasion of personal privacy.

4-5.7 **Exemption 7 (5 USC 552(b)(7)) – Law Enforcement Records**

The following applies to law enforcement records.

- a. *General.* Exemption 7 applies to records compiled for law enforcement purposes but only to the extent that providing these records:
 - Exemption 7(A) – Could reasonably be expected to interfere with enforcement proceedings.
 - Exemption 7(B) – Would deprive a person of a right to a fair trial or impartial adjudication.
 - Exemption 7(C) – Could reasonably be expected to constitute an unwarranted invasion of personal privacy.
 - Exemption 7(D) – Could reasonably be expected to disclose the identity of a confidential source.
 - Exemption 7(E) – Would disclose techniques, procedures, and guidelines used in law enforcement investigations or prosecutions, if the disclosure could reasonably be expected to risk circumvention of the law.
 - Exemption 7(F) – Could reasonably be expected to endanger the life or physical safety of any individual.
- b. *Criminal Law Investigation.* When a request is made that involves access to records covered by exemption 7 and the investigation or proceeding involves a possible violation of criminal law, the Postal Service may treat the records as not subject to FOIA requirements during such time that there is reason to believe that (1) the subject of the investigation or proceeding is not aware of it; and (2) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings.
- c. *Informant Records.* When informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party, the records may be treated as not subject to FOIA requirements unless the informant's status as an informant is officially confirmed.

4-5.8 **Exemption 8 (5 USC 552 (b)(8)) – Financial Institutions**

Exemption 8 applies to information relating to the regulation or supervision of financial institutions and *rarely, if ever applies to Postal Service Records.*

4-5.9 **Exemption 9 (5 USC 552 (b)(9)) – Geological Information**

Exemption 9 applies to geological information on wells and *rarely, if ever applies to Postal Service Records.*

4-6 Fees

4-6.1 General

The Postal Service may charge fees for costs incurred in processing a FOIA request. The requester is responsible for the payment of all fees related to processing the request, even if requested records are not located or are determined to be exempt from disclosure. Requesters must make checks or money orders payable to the “United States Postal Service.”

4-6.2 Aggregate Requests

When a custodian reasonably believes that a requester is attempting to break a request down into a series of requests to avoid fees, the custodian may aggregate the requests and charge accordingly. Multiple requests pertaining to unrelated subject matters are not aggregated. Requests made by more than one requester may be aggregated when a custodian has a concrete basis to conclude that requesters are acting together to avoid fees.

4-6.3 Fee Waivers

- a. *Fees waived for public interest.* The custodian may waive a fee in whole or in part, or any requirement for advance payment, when the custodian determines that providing the records is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the federal government, and is not primarily in the commercial interest of the requester. In determining whether disclosure is in the public interest, all the following factors are considered:
 - (1) The relation of the records to the operations or activities of the Postal Service.
 - (2) The informative value of the information to be disclosed.
 - (3) Any contribution and the significance of that contribution to the public’s understanding of the subject likely to result from disclosure.
 - (4) The nature of the requester’s interest, if any, in the information, including personal or commercial interests.
- b. *Fees waived by officer.* Any Postal Service officer or designee, or the Records Office manager may waive in whole or in part any fee or the requirement for advance payment.

4-6.4 Requester Categories

To assess fees, the custodian must classify requesters into one of the following four categories:-

- a. *Commercial use requesters.* Requesters who are furthering their commercial interests or the commercial interests of those they represent.

- b. *Educational or noncommercial scientific institutions.* Institutions of higher learning, or institutions conducting scientific research not intended to promote a product or industry.
- c. *News media representative.* A requester actively gathering news for an entity that disseminates news to the public (except that media requests for information to further their commercial interests are considered commercial use requests).
- d. *Other.* All other requesters.

4-6.5 How to Assess Fees

- a. *Fees Not Assessed.* The Postal Service does not charge for responding to the following: requests for records if fees do not exceed \$10 or requests for address information as described in section 5-2d.
- b. *Fee Computation.* Fees for each category of requester are computed according to the table below. Fractions of an hour are rounded to the nearest half hour.

Requester Category	Manual Search Time	Computer Search Time	Review Time	Duplication
Commercial Use	\$32 per hour	Compute based on section 4-6.5c	\$32 per hour	\$0.15 per page
Educational/Scientific	None	None	None	1-100 pages free, \$0.15 per page thereafter
News Media	None	None	None	1-100 pages free, \$0.15 per page thereafter
Other Requesters	2 hours free \$32/hour thereafter	First 2 hours free. Compute based on section 4-6.5c	None	1-100 pages free, \$0.15 per page thereafter

- c. *Fees for Computer Searches.* Computer search fees are based on the computer processing and personnel salary rates in the table below. For the “other requester” category, fees should begin to be assessed when the combined cost of computer processing and personnel salaries exceeds the value of 2 salary hours for the level of personnel involved. For example, fees should be assessed when costs exceed \$400 for IT specialist time, \$200 for system or database administrator time, or \$120 for operator time.

Computer processing:

Mainframe usage	\$0.39 per second
Open system usage	\$1.00 per hour
PC usage	\$7 per 15 minutes
Printing computer output	\$0.14 per page
Electronic data delivery	\$100 Setup, plus \$1 gigabyte

Computer personnel:

Operator time	\$60 per hour
System or database administrator time	\$100 per hour
IT specialist time	\$200 per hour (Examples: Database analyst, system programmer, application developer)

- d. *Manual and Computer Searches.* Manual searches include all the time spent looking for responsive material, including page-by-page or line-by-line identification of material within documents. Computer searches include the time required to prepare software for the search. Postal Service may charge for search time even if no responsive records are located or if records located are subsequently determined to be exempt from disclosure.
- e. *Special Fees:*
- (1) *Domestic Special Services.* A copy of one or more of the following is provided upon payment of the fee outlined in *Mailing Standards of the United States Postal Service, Domestic Mail Manual (DMM[®])* section 500: a paid money order; the return receipt requested for mail sent COD, certified, registered, insured; or the domestic delivery record for articles sent COD, certified, registered, or insured. A list of persons who do not want to receive sexually oriented advertising is provided upon payment of the fee listed in DMM section 508.9.4.
 - (2) *Publications.* Publications and other printed materials may be provided at any established price or cost to the Postal Service.
 - (3) *Other Fees.* Other direct costs related to processing a FOIA request that are not accounted for under this section may be assessed upon reasonable documentation to the requester.

4-6.6 **Advance Notice and Payment**

- a. *Advance Notice.* The custodian must notify the requester as soon as reasonably possible 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.
- The custodian should briefly describe the basis for the estimated cost and may offer the requester the opportunity to revise the request to reduce the cost.
- b. *Advance Payment.* Advance payment is required:
- (1) *When the estimated fees are likely to exceed \$250 and the requester has no history of payment.* 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 responding does not run between the date notice requiring advance payment is sent and the date payment is received.

4-6.7 **Accounting for Fees**

Custodians must account for fees as follows:

- a. For fees received at Post Office installations, deposit fees received as Postal Service funds. Record the amounts collected by entries to AIC 198, Freedom of Information Fees.
- b. For fees at non-Post Office installations, forward fees to the disbursing officer at the Eagan Accounting Service Center for deposit. Specify general ledger account 43388, Freedom of Information Fees, as the account for the amounts collected. Send fees to the following address:
DISBURSING OFFICER
EAGAN ACCOUNTING SERVICE CENTER
US POSTAL SERVICE
2825 LONE OAK PKWY
EAGAN MN 55121

4-7 Appeals

4-7.1 **General**

Requesters may appeal decisions to the chief counsel of Customer Programs, at the address in section [1-4.2.11](#). A requester may appeal any of the following:

- a. A request to inspect or copy a record that is denied in whole or in part.
- b. A request for expedited processing that is not approved.
- c. A request for waiver of fees that is not approved.
- d. A request where the custodian makes no determination within the required time.
- e. A request where the custodian provides a “no records” response.

4-7.2 **Time Limit**

The appeal must be sent within 30 days of the date of denial or other action, or within a reasonable time if the appeal is from a failure of the custodian to act. The chief counsel may consider late appeals.

4-7.3 **Required Appeal Elements**

An appeal must include all the following information as applicable:

- a. A copy of the request, any letter of denial or other action, and any other related correspondence.

- b. A statement of the action, or failure to act, from which the appeal is taken.
- c. A statement of the reasons the requester believes the action or failure to act is erroneous.
- d. A statement of the relief sought.
- e. The chief counsel corresponds with the requester in the event all required elements are not included with the appeal. The time period for issuance of a decision in section [4-7.4](#) is stayed pending receipt of all required elements.

4-7.4 **Final Decision**

The decision of the Law Department constitutes the final decision of the Postal Service. The Law Department promptly considers appeals for expedited processing of a request. All other decisions should be made within 20 days (excluding weekends and federal holidays) from receipt of the appeal by the Law Department. The 20-day response period may be extended when reasonably necessary to consider an appeal under one or more of the unusual circumstances described in section [4-3.7c](#). If not prohibited by law, the Law Department may direct disclosure of a record even though disclosure is not required. If the Law Department sustains a denial, the decision must justify why the request was denied and inform the requester of his or her right to judicial review.

4-8 Reporting

Custodians must account for FOIA requests and responses as follows.

4-8.1 **General**

These procedures apply to written requests that are processed under the FOIA and/or the Privacy Act. At the time a response is made, custodians must complete PS Form 8170, *Freedom of Information Act and Privacy Act Request Report*, with the following exceptions:

- a. Requests for individual change of address information under section [5-2d](#).
- b. Requests from federal, state, or local government agencies for any type of information.
- c. Requests from a union, unless the request specifically cites the FOIA or includes the written consent of the records subject authorizing the Postal Service to release records to the union representative.
- d. Any preprinted form, either a Postal Service form or third party form (e.g., from mortgage companies), on which the only reference to the Privacy Act is a Privacy Act notice.

4-8.2 Submissions

FOIA coordinators must submit completed PS Form 8170 to the HQ FOIA RSC. Records custodians must submit completed PS Form 8170 to the appropriate FOIA coordinator as follows:

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
Who are postmasters	FOIA coordinator in the performance cluster

4-8.3 FOIA Annual Report

The Records Office manager submits a report concerning the administration of the FOIA to the Attorney General of the United States annually. The report is available to the public at <http://about.usps.com/who-we-are/foia/annual-foia-reports/welcome.htm>.

This page intentionally left blank

5 Requests for Special Categories of Records

5-1 General

The following procedures apply when responding to requests for certain categories of records that are frequently requested and involve special processing rules. This chapter concerns requests for three 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

Custodians must follow the timetables, fee schedules, reporting requirements, and other administrative requirements set forth in chapter [4](#).

5-2 Requests for Employee or Customer Information

a. *General.*

- (1) If requesters seek records about themselves, the records must be released subject to the following exceptions. If the records are contained in a system of records, the requester is generally entitled to access to the records under the Privacy Act. However, the records should be withheld if they are exempt from disclosure under both the Privacy Act and the FOIA (see sections [3-4.1b\(7\)](#) and [4-5](#)). Typically if there is a Privacy Act exemption there is a FOIA exemption that will apply as well. If the records are not contained in a system of records, then the requester is entitled to access the records under the FOIA. The records must be released unless a FOIA exemption applies.
- (2) If the requester seeks records about another customer, employee, or other individual, privacy rules apply. If the information is contained in a system of records, it may only be released as allowed under the Privacy Act as described in section [3-5](#). Even if not so protected, records about individuals may be exempt from disclosure under one or more FOIA exemptions, particularly Exemption 6 (see section [4-5.6](#)).

Nonpublic or confidential information about business customers or the Postal Service should not be disclosed if exempt, such as under FOIA Exemptions 3 or 4 (see sections [4-5.3](#) and [4-5.4](#)).

- b. *Employee Information.* The following information about employees may be disclosed. Other information may only be disclosed under the general rule above.
 - (1) *Employment Data.* 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.
 - (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.
 - (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 or Social Security numbers).
- 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: (1) 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 (2) 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:
- The custodian determines that the information will not be disclosed.
 - The information lawfully has been published or has been officially made available to the public.
 - Disclosure of the information is required by law (other than FOIA).
 - 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 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 section [4-3.6](#). 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:
- (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.
 - (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:*
 - (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 section [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 party

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 or Caller 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:

- 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.
 - 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.
 - The names of all known parties to the litigation.
 - The court in which the case has been or will be commenced.
 - The docket or other identifying number, if one has been issued.
 - 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 or Caller 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 copy of 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 copy of 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 copy of form.
Subpoena or court order	Only if counsel concurs	Only if counsel concurs	Yes	Only if counsel concurs
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" below. 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 copy of the form. (See exception.*)

Type of Requester	Disclose Boxholder Information from PS Form 1093, <i>Application for Post Office Box or Caller Service</i> (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, <i>Application for Delivery of Mail Through Agent</i> (Both Business and Personal Use)
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

Postmaster _____	Date _____
City, State, ZIP Code _____	
<p>REQUEST FOR CHANGE OF ADDRESS OR BOXHOLDER INFORMATION NEEDED FOR SERVICE OF LEGAL PROCESS</p>	
Please furnish the new address or the name and street address (if a boxholder) for the following:	
Name: _____	
Address: _____	
<p>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.</p>	
<p>The following information is provided in accordance with 39 CFR 265.6(d)(5)(ii). There is no fee for providing boxholder or change of address information.</p>	
<p>1. Capacity of requester (e.g., process server, attorney, party representing self): _____</p>	
<p>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): _____ _____</p>	
<p>3. The names of all known parties to the litigation: _____</p>	
<p>4. The court in which the case has been or will be heard: _____</p>	
<p>5. The docket or other identifying number (a or b must be completed):</p> <p> ___ a. Docket or other identifying number: _____</p> <p> ___ b. Docket or other identifying number has not been issued.</p>	
<p>6. The capacity in which this individual is to be served (e.g., defendant or witness): _____</p>	
<p>WARNING</p>	
<p>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).</p>	
<p>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.</p>	
_____ Signature	_____ Address
_____ Printed Name	_____ City, State, ZIP Code
<p>POST OFFICE USE ONLY</p>	
_____ No change of address order on file.	NEW ADDRESS OR BOXHOLDER'S NAME POSTMARK
_____ Moved, left no forwarding address.	AND STREET ADDRESS
_____ No such address.	_____ _____ _____

Exhibit 5-2c

Address Information Request Format – Government Agencies

(AGENCY LETTERHEAD)	
To:	Postmaster _____
Agency Control Number	_____
Date	_____
ADDRESS INFORMATION REQUEST	
<p>Please furnish this agency with the new address, if available, for the following individual or verify whether or not 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.</p>	
Name:	_____
Last Known Address:	_____
<p>I certify that the address information for this individual is required for the performance of this agency's official duties.</p>	

(Signature of Agency Official)	

(Title)	
FOR POST OFFICE USE ONLY	
<input type="checkbox"/> MAIL IS DELIVERED TO ADDRESS GIVEN	NEW ADDRESS
<input type="checkbox"/> NOT KNOWN AT ADDRESS GIVEN	_____
<input type="checkbox"/> MOVED, LEFT NO FORWARDING ADDRESS	_____
<input type="checkbox"/> NO SUCH ADDRESS	
<input type="checkbox"/> OTHER (SPECIFY):	BOXHOLDER STREET ADDRESS
_____	_____
_____	_____
Agency return address	Postmark/Date Stamp

5-3 Congressional Requests

If the request is on behalf of Congress through a committee or subcommittee, disclosure is the general rule. In most cases, only Executive privilege could justify nondisclosure. Consult appropriate counsel. Process all other Congressional requests as a request from any person under the procedures in chapter 4. Forward all Congressional requests for nonpublic records to:

SENIOR VICE PRESIDENT GOVERNMENT RELATIONS
US 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 legal counsel. Records may only be released on advice of counsel. Postal Service regulations concerning providing records subject to legal proceedings are contained in 39 CFR 265.11-13.

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 section [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			
<p>[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.</p>			
<p>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.</p>			
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

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

100.000	General Personnel Records
100.100	Recruiting, Examining, and Placement Records
100.200	Employee Performance Records
100.300	Employee Development and Training Records
100.400	Personnel Compensation and Payroll Records
100.500	Personnel Resource Management Records
100.600	Personnel Research Records
100.700	Medical Records
100.800	Employee Accident Records
100.850	Office of Workers' Compensation Program (OWCP) Record Copies

100.900	Employee Inquiry, Complaint, and Investigative Records
100.950	Employee Assistance Program (EAP) Records
200.000	Labor Relations Records
300.000	Finance Records
400.000	Supplier and Tenant Records
500.000	Property Management Records
500.050	HSPD-12: Identity Management System
500.100	Carrier and Vehicle Operator Records
500.200	Controlled Correspondence, FOIA, and Privacy Act Disclosure Records
500.300	Emergency Management Records
600.000	Legal Records Related to Mail
600.100	General Legal Records
600.200	Privacy Act and FOIA Appeal and Litigation Records
600.300	Public and Confidential Financial Disclosure Reports
600.400	Administrative Litigation Records
600.500	Judicial Officer Records
700.000	Inspection Service Investigative File System
700.100	Mail Cover Program Records
700.200	Vehicular Violations Records Systems
700.300	Inspector General Investigative Records

Part II. Customer Systems

800.000	Address Change, Mail Forwarding, and Related Services
800.100	Address Matching for Mail Processing
800.200	Address Element Correction Enhanced Service (AECES)
810.100	www.usps.com Registration
810.200	www.usps.com Ordering, Payment, and Fulfillment
810.300	Offline Registration, Payment, and Fulfillment
820.100	Mailer Services — Applications and Approvals
820.200	Mail Management and Tracking Activity
830.000	Customer Service and Correspondence
840.000	Customer Mailing and Delivery Instructions
850.000	Auction Files
860.000	Financial Transactions
870.100	Trust Funds and Transaction Records
870.200	Meter Postage and PC Postage Customer Data and Transaction Records
880.000	Post Office and Retail Services
890.000	Sales, Marketing, Events, and Publications
900.000	International Services
910.000	Identity and Document Verification Services

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.

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

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

USPS 100.000

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.

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, date(s) of birth, postal assignment information, work contact information, home address(es) and phone number(s), finance number(s), duty location, and pay location.
2. *Compensation and payroll information:* Records related to payroll, 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.

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.

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 approved monetary awards are retained 7 years. Records of award submissions not approved are retained 90 days.

4. Automated records of employee ideas are maintained for 7 years.
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.

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 100.500

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.

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 (USPS employees, other federal agency employees, or contract employees) involved in EEO discrimination complaints.
2. USPS employees involved in labor arbitration.
3. USPS employees who are candidates considered by promotion boards for an EEO staff position.
4. Individuals and organizations interested in providing alternative dispute resolution (ADR) services to all disputes, except those arising under USPS collective bargaining agreements.

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, 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. *EEO staff position information:* Records related to candidates for EEO staff positions, including name, Social Security Number, Employee Identification Number, date of birth, postal assignment information, work contact information, finance number(s), duty location, and pay location.
4. *ADR provider information:* Records related to ADR providers 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 accomplish EEO staff selection.
4. To determine ADR service provider 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.

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. 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

For EEO discrimination complaint case records, labor arbitration records, EEO staff selection records, and REDRESS ADR staff

providers: Vice President, Labor Relations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

For records of non-REDRESS ADR staff providers: General Counsel and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Notification Procedure

Inquiries about EEO discrimination complaint case records must be submitted to the EEO officer at the district, area, or Headquarters level, and must include complainant name, complainant Social Security Number or Employee Identification Number, location, and case number and year. Inquiries about labor arbitration records and ADR provider records must be submitted to the system manager. Inquiries about EEO staff selection records must be addressed to the head of the facility where application was made.

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 EEO staff position records: employee applicant and other systems of records. For ADR provider records, the 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. *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 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 to 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.

systems are incorporated into this system, the exemptions applicable to the original primary system continue to apply to the incorporated records.

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

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 login 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 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, www.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, www.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, www.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, in writing, or via telephone. 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, e-mail 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 provide address information to the American Red Cross or other disaster relief organization about a customer who has been relocated because of disaster.
4. To support investigations related to law enforcement for fraudulent 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. 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 e-mail 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, 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 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 800.100

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 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 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 www.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; home and business phone and fax number; e-mail; URL; and Automated Clearing House (ACH) information.
2. *Identity verification information:* Question, answer, username, user ID, and password.
3. *Business specific information:* Business type and location, business IDs, annual revenue, number of employees, industry, nonprofit rate status, product usage information, annual and/or monthly shipping budget, payment method and information, planned use of product, and age of Web site.
4. *Customer preferences:* Preferences to receive USPS marketing information, preferences to receive marketing information from USPS partners, preferred means of contact, preferred e-mail 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, 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 obtain accurate contact information in order to deliver requested products, services, and other material.
3. To authenticate customer logon information for www.usps.com.
4. To permit customer feedback in order to improve www.usps.com or USPS 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 database, computer storage media, and paper.

Retrievability

By customer name, customer ID(s), phone number, or mail or e-mail 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.

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 Marketing/Sales 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 *www.usps.com*.

Categories of Records in the System

1. *Customer information:* Name, customer ID(s), phone and/or fax number, mail address and e-mail 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 and export control purposes.
7. To satisfy statistical reporting requirements for foreign trade.

Routine Uses of Records in the System, Including Categories of Users and the Purposes of Such Uses

Records may be disclosed to the Office of Foreign Assets Control, the Bureau of Industry and Security, and other government authorities charged with enforcing export control laws, rules, and policies, including 50 U.S.C. 1702.

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 e-mail 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. Records related to shipping services and domestic and international labels are retained up to 90 days. Delivery Confirmation and return receipt records are retained for 6 months. Signature Confirmation records are retained for 1 year. ACH records are retained for up to 2 years.
2. 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.
3. Other records related to shipping services and domestic and international labels are retained up to 90 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 Marketing/Sales Officer, 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; 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), and cellphone 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 business mailers with information about the status of mailings within the USPS mail processing network.
5. To help mailers identify performance issues regarding their mail.
6. 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.

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

President, Digital Solutions, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Chief Information Officer, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Chief Marketing/Sales 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 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.

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. 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

Vice President, Consumer and Industry Affairs, 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 Meter and PC Postage Customer Data and Transaction Records.

System Location

USPS Headquarters Marketing, 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; company name; and change of address information.
2. *Identification information:* Customer ID(s), date of device installation, device ID number, device model number, and certificate serial number.

Authority for Maintenance of the System

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

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.

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 4 years after a customer ceases using a postage evidencing system.

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 inquiries 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, 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 ensure accurate and secure mail delivery.
3. 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

President and Chief Marketing/Sales Officer, 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, Global Business, 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 www.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, and contact information.
2. Name and address of senders and addressees.
3. *Information pertaining to mailings:* Contents, order number, volume, destination, weight, origin, value, date, postage and fees, type of mailing, and applicable citation or legend required by the Foreign Trade Regulations.
4. Customer barcode scan data.
5. Company name; contact name, title, and phone and fax number; mail and e-mail 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 satisfy reporting requirements for customs and export control purposes.
5. To satisfy statistical reporting requirements for foreign trade.

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 officials pursuant to Section 343(a) of the Trade Act of 2002, P.L. 107–210, and international agreements or regulations.
- b. Records may be disclosed to the Office of Foreign Assets Control, the Bureau of Industry and Security, and other government authorities charged with 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

Vice President, Global Business, 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

Customers who apply for identity and document verification services.

Categories of Records in the System

1. *Customer information:* Name, address, customer ID(s), telephone number, mail and e-mail address, date of birth, place of birth, company name, title, role, and employment status.
2. Names and contact information of users who are authorized to have access to data.
3. *Verification and payment information:* Credit and/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 (SSN) and credit and/or debit card information are collected, but not stored, in order to verify ID.)
4. Biometric information including fingerprint, photograph, height, weight, and iris scans. (*Note:* Information may be collected, secured, and returned to customer or third parties at the direction of the customer, but not stored.)
5. *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.
6. *Transaction information:* Clerk signature; transaction type, date and time, location, source of transaction; product use and inquiries.
7. Electronic information related to encrypted or hashed documents.

Authority for Maintenance of the System

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

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.

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.

Privacy Act Systems of Records

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 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

1.			E	VG	G	F	P
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)	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b.	To get information about USPS <i>policies</i> regarding privacy	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c.	To get information about USPS <i>procedures</i> regarding privacy (including the Privacy Act)	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d.	To get general Freedom of Information Act (FOIA) information (e.g., how to make or process a FOIA request)	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e.	To get information about FOIA procedures	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f.	To get System of Records (SOR) Information	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g.	Other (specify) _____	<input type="checkbox"/> Yes → <input type="checkbox"/> No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		E	VG	G	F	P	NU
2.	What is your overall impression of the handbook?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.	How would you rate the organization of the handbook?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.	How would you rate the usefulness of the exhibits?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	How would you rate the handbook at providing the information you were seeking?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.	Please rate the following sections:						
a.	Introduction (pages 1-5)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b.	Laws, Guidelines, and Policies (pages 7-26)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c.	Privacy Procedures (pages 11-26)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d.	Freedom of Information Act Procedures (pages 27-47)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e.	System of Records (appendix)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	How would you rate USPS on its privacy protections?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	How would you rate your level of comfort in trusting the USPS not to share personal information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	Did you use this handbook as a USPS employee, USPS business customer, or USPS residential customer? (Mark all that apply) <input type="checkbox"/> USPS Employee <input type="checkbox"/> Business Customer <input type="checkbox"/> Residential Customer						
10.	In your opinion, does the handbook contain: <input type="checkbox"/> Too much information <input type="checkbox"/> Just the right amount of information <input type="checkbox"/> Not enough information						
11.	In your opinion, was the handbook: <input type="checkbox"/> Easy to understand <input type="checkbox"/> Somewhat easy to understand <input type="checkbox"/> Difficult to understand						

12.		Very Likely	Likely	Not Likely
How likely are you to use this handbook again to answer any future questions about:				
	Privacy issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	FOIA information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	USPS procedures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

