

the demand and for legal work in connection with the demand; expenses generated by equipment used to search for, produce, and copy the requested information; travel costs of the employee and the agency attorney, including lodging and per diem where appropriate. Such fees shall be assessed at the rates and in the manner specified in §265.9.

(ii) At the discretion of the Inspection Service where appropriate, fees and costs may be estimated and collected before testimony is given.

(iii) The provisions in this section do not affect rights and procedures governing public access to official documents pursuant to the Freedom of Information Act, 5 U.S.C 552a.

(1) *Acceptance of service.* The rules in this section in no way modify the requirements of the Federal Rules of Civil Procedure (28 U.S.C. Appendix) regarding service of process.

[60 FR 36712, July 18, 1995, as amended at 69 FR 34935, June 23, 2004]

APPENDIX A TO PART 265—FEES FOR COMPUTER SEARCHES

When requested information must be retrieved by computer, fees charged to the requester are based on rates for personnel and computer time. Estimates are provided to the requester in advance and are based on the following rates:

	Price	Unit
Personnel:		
High technical	\$120	per hour.
Medium technical	70	per hour.
Low technical	50	per hour.
Computer Processing:		
Mainframe usage39	per second.
Midrange server usage06	per second.
PC usage	7.00	per 15 minutes.
Printing computer output14	per page.
Magnetic tape production	24.00	per volume.

[68 FR 56559, Oct. 1, 2003]

PART 266—PRIVACY OF INFORMATION

Sec.

- 266.1 Purpose and scope.
- 266.2 Policy.
- 266.3 Responsibility.
- 266.4 Collection and disclosure of information about individuals.
- 266.5 Notification.
- 266.6 Procedures for requesting inspection, copying, or amendment of records.

- 266.7 Appeal procedure.
- 266.8 Schedule of fees.
- 266.9 Exemptions.
- 266.10 Computer matching.

AUTHORITY: 39 U.S.C. 401; 5 U.S.C. 552a.

§266.1 Purpose and scope.

This part is intended to protect individual privacy and affects all personal information collection and usage activities of the entire U.S. Postal Service. This includes the information interface of Postal Service employees to other employees, to individuals from the public at large, and to any private organization or governmental agency.

[40 FR 45723, Oct. 2, 1975]

§266.2 Policy.

It is the policy of the U.S. Postal Service to ensure that any record within its custody that identifies or describes any characteristic or provides historical information about an individual or that affords a basis for inferring personal characteristics, or things done by or to such individual, including the record of any affiliation with an organization or activity, or admission to an institution, is accurate, complete, timely, relevant, and reasonably secure from unauthorized access. Additionally, it is the policy to provide the means for individuals to know: (a) Of the existence of all Postal Service Privacy Act systems of records, (b) the recipients and usage made of such information, (c) what information is optional or mandatory to provide to the Postal Service, (d) the procedures for individuals to review and request update to all information maintained about themselves, (e) the reproduction fees for releasing records, (f) the procedures for individual legal appeal in cases of dissatisfaction; and (g) of the establishment or revision of a computer matching program.

[45 FR 44272, July 1, 1980, as amended at 59 FR 37160, July 21, 1994]

§266.3 Responsibility.

- (a) *Records Office.* The Records Office, within the Privacy Office, will ensure Postal Service-wide compliance with this policy.
- (b) *Custodian.* Custodians are responsible for adherence to this part within

United States Postal Service

§ 266.4

their respective units and in particular for affording individuals their rights to inspect and obtain copies of records concerning them.

(c) *Information System Executive.* These managers are responsible for reporting to the Records Office the existence or proposed development of Privacy Act systems of records. They also must report any change that would alter the systems description as published in the FEDERAL REGISTER. They establish the relevancy of the information within those systems.

(d) *Data Integrity Board*—(1) *Responsibilities.* The Data Integrity Board oversees Postal Service computer matching activities. Its principal function is to review, approve, and maintain all written agreements for use of Postal Service records in matching programs to ensure compliance with the Privacy Act and all relevant statutes, regulations, and guidelines. In addition, the Board annually reviews matching programs and other matching activities in which the Postal Service has participated during the preceding year to determine compliance with applicable laws, regulations, and agreements; compiles a biennial matching report of matching activities; and performs review and advisement functions relating to records accuracy, recordkeeping and disposal practices, and other computer matching activities.

(2) *Composition.* The Privacy Act requires that the senior official responsible for implementation of agency Privacy Act policy and the Inspector General serve on the Board. The Chief Privacy Officer, as administrator of Postal Service Privacy Act policy, serves as Secretary of the Board and performs the administrative functions of the Board. The Board is composed of these and other members designated by the Postmaster General, as follows:

- (i) Vice President and Consumer Advocate (Chairman).
- (ii) Chief Postal Inspector.
- (iii) Inspector General.
- (iv) Senior Vice President, Human Resources.
- (v) Vice President, General Counsel.

- (vi) Chief Privacy Officer.

[40 FR 45723, Oct. 2, 1975, as amended at 45 FR 44272, July 1, 1980; 59 FR 37160, July 21, 1994; 60 FR 57345, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003]

§ 266.4 Collection and disclosure of information about individuals.

(a) The following rules govern the collection of information about individuals throughout Postal Service operations;

- (1) The Postal Service will:

- (i) Collect, solicit and maintain only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or Executive Order,

- (ii) Collect information, to the greatest extent practicable, directly from the subject individual when such information may result in adverse determinations about an individual's rights, benefits or privileges,

- (iii) Inform any individual who has been asked to furnish information about himself whether that disclosure is mandatory or voluntary, by what authority it is being solicited, the principal purposes for which it is intended to be used, the routine uses which may be made of it, and any penalties and specific consequences for the individual, which are known to the Postal Service, which will result from refusal to furnish it.

- (2) The Postal Service will not discriminate against any individual who fails to provide information about himself unless that information is required or necessary for the conduct of the system or program in which the individual desires to participate.

- (3) No information will be collected (or maintained) describing how individuals exercise rights guaranteed by the First Amendment unless the Postmaster General specifically determines that such information is relevant and necessary to carry out a statutory purpose of the Postal Service.

- (4) The Postal Service will not require individuals to furnish their Social Security account number or deny a right, privilege or benefit because of an individual's refusal to furnish the number unless it must be provided by Federal law.

§ 266.4

39 CFR Ch. I (7-1-13 Edition)

(b) *Disclosures*—(1) *Disclosure: Limitations On.* The Postal Service will not disseminate information about an individual unless reasonable efforts have been made to assure that the information is accurate, complete, timely and relevant and unless:

(i) The individual to whom the record pertains has requested in writing that the information be disseminated, or

(ii) It has obtained the prior written consent of the individual to whom the record pertains, or

(iii) The dissemination is in accordance with paragraph (b)(2) of this section.

(2) Dissemination of personal information may be made:

(i) To a person pursuant to a requirement of the Freedom of Information Act (5 U.S.C. 552);

(ii) To those officers and employees of the Postal Service who have a need for such information in the performance of their duties;

(iii) For a routine use as contained in the system notices published in the FEDERAL REGISTER;

(iv) To a recipient who has provided advance adequate written assurance that the information will be used solely as a statistical reporting or research record, and to whom the information is transferred in a form that is not individually identifiable;

(v) To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13, U.S.C.;

(vi) To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

(vii) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if upon such disclosure notification is transmitted to the last known address of such individual;

(viii) To a federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, if

such activity is authorized by law and if the head of the agency or instrumentality has made a written request to the Postal Service specifying the particular portion of the record desired and the law enforcement activity for which the record is sought;

(ix) To either House of Congress or its committees or subcommittees to the extent of matter within their jurisdiction;

(x) To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office;

(xi) Pursuant to the order of a court of competent jurisdiction.

(3) *Names and Addresses of Postal Customers.* The disclosure of lists of names or addresses of Postal customers or other persons to the public is prohibited (39 U.S.C. 412). Names or addresses will be disclosed only in those cases permitted by 39 CFR 265.6(d) relating to the Release of Information.

(4) *Employee Credit References.* A credit bureau or commercial firm from which an employee is seeking credit may be given the following information upon request: grade, duty status, length of service, job title, and salary.

(5) *Employee Job References.* Prospective employers of a postal employee or a former postal employee may be furnished with the information in paragraph (b)(4) of this section, in addition to the date and the reason for separation, if applicable. 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 additional information is desired, the requester must submit the written consent of the employee, and an accounting of the disclosure must be kept.

(6) *Computer matching purposes.* Records from a Postal Service system of records may be disclosed to another agency for the purpose of conducting a computer matching program or other matching activity as defined in paragraphs (c) and (d) of §262.5, but only after a determination by the Data Integrity Board that the procedural requirements of the Privacy Act, the

guidelines issued by the Office of Management and Budget, and these regulations as may be applicable are met. These requirements include:

(i) *Routine use.* Disclosure is made only when permitted as a routine use of the system of records. The Manager, Records Office, determines the applicability of a particular routine use and the necessity for adoption of a new routine use.

(ii) *Notice.* Publication of new or revised matching programs in the FEDERAL REGISTER and advance notice to Congress and the Office of Management and Budget must be made pursuant to paragraph (f) of § 266.5.

(iii) *Computer matching agreement.* The participants in a computer matching program must enter into a written agreement specifying the terms under which the matching program is to be conducted (see § 266.10). The Manager, Records Office, may require that other matching activities be conducted in accordance with a written agreement.

(iv) *Data Integrity Board approval.* No record from a Postal Service system of records may be disclosed for use in a computer matching program unless the matching agreement has received approval by the Postal Service Data Integrity Board (see § 266.10). Other matching activities may, at the discretion of the Manager, Records Office, be submitted for Board approval.

(c) *Correction Disclosure.* Any person or other agency to which a personal record has been or is to be disclosed shall be informed of any corrections or notations of dispute relating thereto affecting the accuracy, timeliness or relevance of that personal record.

(d) *Recording of Disclosure.* (1) An accurate accounting of each disclosure will be kept in all instances except those in which disclosure is made to the subject of the record, or to Postal Service employees in the performance of their duties or is required by the Freedom of Information Act (5 U.S.C. 552).

(2) The accounting will be maintained for at least five (5) years or the life of the record, whichever is longer.

(3) The accounting will be made available to the individual named in the record upon inquiry, except for disclosures made pursuant to provision

paragraph (b)(2)(viii) of this section relating to law enforcement activities.

[40 FR 45723, Oct. 2, 1975, as amended at 45 FR 44272, July 1, 1980; 58 FR 62036, Nov. 24, 1993; 59 FR 37160, July 21, 1994; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003]

§ 266.5 Notification.

(a) *Notification of Systems.* Upon written request, the Postal Service will notify any individual whether a specific system named by the individual contains a record pertaining to him or her. See § 266.6 for suggested form of request.

(b) *Notification of Disclosure.* The Postal Service shall make reasonable efforts to serve notice on an individual before any personal information on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

(c) *Notification of Amendment.* (See § 266.6(c)(1) relating to amendment of records upon request.)

(d) *Notification of New Use.* Any newly intended use of personal information maintained by the Postal Service will be published in the FEDERAL REGISTER thirty (30) days before such use becomes operational. Public views may then be submitted to the Records Office.

(e) *Notification of Exemptions.* The Postal Service will publish within the FEDERAL REGISTER its intent to exempt any system of records and shall specify the nature and purpose of that system.

(f) *Notification of computer matching program.* The Postal Service publishes in the FEDERAL REGISTER and forwards to Congress and the Office of Management and Budget advance notice of its intent to establish, substantially revise, or renew a matching program, unless such notice is published by another participant agency. In those instances in which the Postal Service is the "recipient" agency, as defined in the Act, but another participant agency sponsors and derives the principal benefit from the matching program, the other agency is expected to publish the notice. The notice must be sent to Congress and OMB 40 days, and published at least thirty (30) days, prior to (1) initiation of any matching activity under

§ 266.6

39 CFR Ch. I (7–1–13 Edition)

a new or substantially revised program, or (2) expiration of the existing matching agreement in the case of a renewal of a continuing program.

[40 FR 45724, Oct. 2, 1975; 40 FR 48512, Oct. 16, 1975, as amended at 45 FR 44272, July 1, 1980; 59 FR 37161, July 21, 1994; 60 FR 57345, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003; 69 FR 34935, June 23, 2004]

§ 266.6 Procedures for requesting inspection, copying, or amendment of records.

The purpose of this section is to provide procedures by which an individual may have access and request amendment to personal information within a Privacy Act System of Records.

(a) *Submission of Requests*—(1) *Manner of submission*. Inquiries regarding the contents of records systems or access or amendment to personal information should be submitted in writing to the custodian of the official record, if known, or to the Manager, Records Office, U.S. Postal Service, 475 L'Enfant Plaza SW., Washington, DC 20260, telephone (202) 268–2608. Requests submitted to the Office of Inspector General should be submitted to the Freedom of Information Act/Privacy Officer, Office of Inspector General, 1735 North Lynn Street, Arlington, Virginia, 22209–2020. Inquiries should be clearly marked, “Privacy Act Request”. Any inquiry concerning a specific system of records should provide the Postal Service with the information contained under “Notification” for that system as published in the FEDERAL REGISTER. If the information supplied is insufficient to locate or identify the record, the requester will be notified promptly and, if possible, informed of additional information required. If the requester is not a Postal Service employee, he should designate the post office at which he wishes to review or obtain copies of records. Amendment requests contest the relevance, accuracy, timeliness or completeness of the record and will include a statement of the amendment requested.

(2) *Third party inquiries*. Anyone desiring to review or copy records pertaining to another person must have the written consent of that person.

(3) *Period for response by custodian*. Upon receipt of an inquiry, the custodian will respond with an acknowledgment of receipt within ten (10) days. If the inquiry requires the custodian to determine whether a particular record exists, the inquirer shall be informed of this determination as a part of the acknowledgment letter.

(b) *Compliance with Request for Access*—(1) *Notification of time and place for inspection*. When a requested record has been identified and is to be disclosed, the custodian shall ensure that the record is made available promptly and shall immediately notify the requester where and when the record will be available for inspection or copying. Postal Service records will normally be available for inspection and copying during regular business hours at the postal facilities at which they are maintained. The custodian may, however, designate other reasonable locations and times for inspection and copying of some or all of the records within his custody.

(2) *Identification of requester*. The requester must present personal identification sufficient to satisfy the custodian as to his identity prior to record review. Examples of sufficient identification are a valid driver's license, Medicare card, and employee identification cards.

(3) *Responsibilities of requester*. The requester shall assume the following responsibilities regarding the review of official personal records:

(i) Requester must agree not to leave Postal Services premises with official records unless specifically given a copy for that purpose by the custodian or his representative.

(ii) Requester must sign a statement indicating he has reviewed a specific record(s) or category of record.

(iii) Requester may be accompanied by a person he so chooses to aid in the inspection of information; however, requester must furnish the Postal Service with written authorization for such review in that person's presence.

(4) *Special rules for medical records*. A medical record shall be disclosed to the requester to whom it pertains unless, in the judgment of the medical officer, access to such record could have an adverse effect upon such individual. When

United States Postal Service

§ 266.8

the medical officer determines that the disclosure of medical information could have an adverse effect upon the individual to whom it pertains, the medical officer will transmit such information to a medical doctor named by the requesting individual.

(5) *Limitations on access.* Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding. Other limitations on access are those specifically addressed in §§ 266.6(b)(4) and 266.9.

(6) *Response when compliance is not possible.* A reply denying a written request to review a record shall be in writing signed by the custodian or other appropriate official and shall be made only if such a record does not exist or does not contain personal information relating to the requester, or is exempt from disclosure. This reply shall include a statement regarding the determining factors of denial, and the right to appeal to denial to the General Counsel.

(c) *Compliance With Request for Amendment.* (1) Correct or eliminate any information that is found to be incomplete, inaccurate, not relevant to a statutory purpose of the Postal Service, or not timely and notify the requester when this action is complete, or

(2) Not later than thirty (30) working days after receipt of a request to amend, notify the requester of a determination not to amend and of the requester's right to appeal, or to submit, in lieu of an appeal, a statement of reasonable length setting forth a position regarding the disputed information to be attached to the contested personal record.

(d) *Availability of Assistance in Exercising Rights.* The Manager, Records Office is available to provide an individual with assistance in exercising rights pursuant to this part.

[40 FR 45723, Oct. 2, 1975, as amended at 45 FR 44272, July 1, 1980; 51 FR 26386, July 23, 1986; 60 FR 57345, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 67 FR 16024, Apr. 4, 2002; 68 FR 56560, Oct. 1, 2003]

§ 266.7 Appeal procedure.

(a) *Appeal Procedure.* (1) If a request to inspect, copy, or amend a record is

denied, in whole or in part, or if no determination is made within the period prescribed by this part, the requester shall appeal to the General Counsel, U.S. Postal Service, Washington, DC 20260-1100.

(2) The requester should submit his appeal in writing within thirty (30) days of the date of denial, or within ninety (90) days of such request if the appeal is from a failure of the custodian to make a determination. The letter of appeal should include, as applicable:

(i) Reasonable identification of the record access to which or the amendment of which was requested.

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

(iii) A copy of the request, of the notification of denial and of any other related correspondence.

(3) Any record found on appeal to be incomplete, inaccurate, not relevant, or not timely, shall within thirty (30) working days of the date of such findings be appropriately amended.

(4) The decision of the General Counsel, constitutes the final decision of the Postal Service on the right of the requester to inspect, copy, change, or update a record. The decision on the appeal shall be in writing and in the event of a denial shall set forth the reasons for such denial and state the individual's right to obtain judicial review in a district court. An indexed file of decisions on appeals shall be maintained by the General Counsel.

(b) *Submission of Statement of Disagreement.* If the final decision concerning a request for the amendment of a record does not satisfy the requester, any statement of reasonable length provided by that individual setting forth a position regarding the disputed information will be accepted and attached to the relevant personal record.

[40 FR 45723, Oct. 2, 1975, as amended at 41 FR 24709, June 18, 1976; 45 FR 44273, July 1, 1980; 51 FR 26386, July 23, 1986; 60 FR 57345, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003]

§ 266.8 Schedule of fees.

(a) *Policy.* The purpose of this section is to establish fair and equitable fees to

§ 266.9

39 CFR Ch. I (7-1-13 Edition)

permit duplication of records for subject individuals (or authorized representatives) while recovering the full allowable direct costs incurred by the Postal Service.

(b) *Duplication.* (1) For duplicating any paper or micrographic record or publication or computer report, the fee is \$.15 per page, except that the first 100 pages furnished in response to a particular request shall be furnished without charge. See paragraph (d) of this section for fee limitations.

(2) The Postal Service may at its discretion make coin-operated copy machines available at any location. In that event, requesters will be given the opportunity to make copies at their own expense.

(3) The Postal Service normally will not furnish more than one copy of any record. If duplicate copies are furnished at the request of the requester, \$.15 per page fee is charged for each copy of each duplicate page without regard to whether the requester is eligible for free copies pursuant to § 266.8(b)(1).

(c) *Aggregating requests.* When the custodian reasonably believes that a requester is attempting to break a request for similar types of records down into a series of requests in order to evade the assessment of fees, the custodian may aggregate the requests and charge accordingly.

(d) *Limitations.* No fee will be charged an individual for the process of retrieving, reviewing, or amending a record pertaining to that individual.

(e) The Postal Service may, at its discretion, require reimbursement of its costs as a condition of participation in a computer matching program or activity with another agency. The agency to be charged is notified in writing of the approximate costs before they are incurred. Costs are calculated in accordance with the schedule of fees at § 265.9.

[52 FR 38230, Oct. 15, 1987, as amended at 59 FR 37161, July 21, 1994; 68 FR 56560, Oct. 1, 2003]

§ 266.9 Exemptions.

(a) Subsections 552a(j) and (k) of 5 U.S.C. 552a empower the Postmaster General to exempt systems of records meeting certain criteria from various

other subsections of 5 U.S.C. 552a. With respect to systems of records so exempted, nothing in this part shall require compliance with provisions hereof implementing any subsections of 5 U.S.C. 552a from which those systems have been exempted.

(b) Paragraph (b)(1) of this section contains a summary of provisions of 5 U.S.C. 552a for which exemption is claimed for some systems of records pursuant to, and to the extent permitted by, subsections 552a(j) and (k) of 5 U.S.C. 552a. Paragraphs (b)(2) through (5) of this section identify the exempted systems of records, the exemptions applied to each, and the reasons for the exemptions:

(1) *Explanation of provisions under 5 U.S.C. 552a for which an exemption is claimed in the systems discussed below.* (i) Subsection (c)(3) requires an agency to make available to the individual named in the records an accounting of each disclosure of records.

(ii) Subsection (c)(4) requires an agency to inform any person or other agency to which a record has been disclosed of any correction or notation of dispute the agency has made to the record in accordance with 5 U.S.C. 552a(d).

(iii) Subsections (d)(1) through (4) require an agency to permit an individual to gain access to records about the individual, to request amendment of such records, to request a review of an agency decision not to amend such records, and to provide a statement of disagreement about a disputed record to be filed and disclosed with the disputed record.

(iv) Subsection (e)(1) requires an agency to maintain in its records only such information about an individual that is relevant and necessary to accomplish a purpose required by statute or executive order of the President.

(v) Subsection (e)(2) requires an agency to collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.

(vi) Subsection (e)(3) requires an agency to inform each person whom it

asks to supply information of the authority under which the information is sought, the purposes for which the information will be used, the routine uses that may be made of the information, whether disclosure is mandatory or voluntary, and the effects of not providing the information.

(vii) Subsection (e)(4)(G) and (H) requires an agency to publish a FEDERAL REGISTER notice of its procedures whereby an individual can be notified upon request whether the system of records contains information about the individual, how to gain access to any record about the individual contained in the system, and how to contest its content.

(viii) Subsection (e)(5) requires an agency to maintain its records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any determination about the individual.

(ix) Subsection (e)(8) requires an agency to make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

(x) Subsection (f) requires an agency to establish procedures whereby an individual can be notified upon request if any system of records named by the individual contains a record pertaining to the individual, obtain access to the record, and request amendment.

(xi) Subsection (g) provides for civil remedies if an agency fails to comply with the access and amendment provisions of subsections (d)(1) and (d)(3), and with other provisions of 5 U.S.C. 552a, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.

(xii) Subsection (m) requires an agency to cause the requirements of 5 U.S.C. 552a to be applied to a contractor operating a system of records to accomplish an agency function.

(2) Pursuant to subsection 552a(j)(2), *Emergency Management Records, USPS 500.300; Inspection Service Investigative File System, USPS 700.000; Mail Cover Program Records, USPS 700.100; and Inspector General Investigative Records, USPS 700.300*, are exempt from sub-

sections 552a (c)(3), (c)(4), (d)(1)–(4), (e)(1)–(3), (e)(4) (G) and (H), (e)(5), (e)(8), (f), (g), and (m) because the systems contain information pertaining to the enforcement of criminal laws. The reasons for exemption follow:

(i) Disclosure to the record subject pursuant to subsections (c)(3), (c)(4), or (d)(1)–(4) could:

(A) Alert subjects that they are targets of an investigation or mail cover by the Postal Inspection Service or an investigation by the Office of Inspector General;

(B) Alert subjects of the nature and scope of the investigation and of evidence obtained;

(C) Enable the subject of an investigation to avoid detection or apprehension;

(D) Subject confidential sources, witnesses, and law enforcement personnel to harassment or intimidation if their identities were released to the target of an investigation;

(E) Constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation;

(F) Intimidate potential witnesses and cause them to be reluctant to offer information;

(G) Lead to the improper influencing of witnesses, the destruction or alteration of evidence yet to be discovered, the fabrication of testimony, or the compromising of classified material; and

(H) Seriously impede or compromise law enforcement, mail cover, or background investigations that might involve law enforcement aspects as a result of the above.

(ii) Application of subsections (e)(1) and (e)(5) is impractical because the relevance, necessity, or correctness of specific information might be established only after considerable analysis and as the investigation progresses. As to relevance (subsection (e)(1)), effective law enforcement requires the keeping of information not relevant to a specific Postal Inspection Service investigation or Office of Inspector General investigation. Such information may be kept to provide leads for appropriate law enforcement and to establish patterns of activity that might relate to the jurisdiction of the Office of

Inspector General, Postal Inspection Service, and/or other agencies. As to accuracy (subsection (e)(5)), the correctness of records sometimes can be established only in a court of law.

(iii) Application of subsections (e)(2) and (e)(3) would require collection of information directly from the subject of a potential or ongoing investigation. The subject would be put on alert that he or she is a target of an investigation by the Office of Inspector General, or an investigation or mail cover by the Postal Inspection Service, enabling avoidance of detection or apprehension, thereby seriously compromising law enforcement, mail cover, or background investigations involving law enforcement aspects. Moreover, in certain circumstances the subject of an investigation is not required to provide information to investigators, and information must be collected from other sources.

(iv) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply because this system is exempt from the provisions of subsection (d). Nevertheless, the Postal Service has published notice of its notification, access, and contest procedures because access is appropriate in some cases.

(v) Application of subsection (e)(8) could prematurely reveal an ongoing criminal investigation to the subject of the investigation.

(vi) The provisions of subsection (g) do not apply because exemption from the provisions of subsection (d) renders the provisions on suits to enforce subsection (d) inapplicable.

(vii) If one of these systems of records is operated in whole or in part by a contractor, the exemptions claimed herein shall remain applicable to it (subsection (m)).

(3) Pursuant to subsection 552a(k)(2), *Labor Relations Records, USPS 200.000; Emergency Management Records, USPS 500.300; Inspection Service Investigative File System, USPS 700.000; Mail Cover Program Records, USPS 700.100; Inspector General Investigative Records, USPS 700.300; and Financial Transactions, USPS 860.000*, are exempt from certain subsections of 5 U.S.C. 552a because the systems contain investigatory material compiled for law enforcement purposes

other than material within the scope of subsection 552a(j)(2).

(i) *Emergency Management Records, USPS 500.300; Inspection Service Investigative File System, USPS 700.000; Mail Cover Program Records, USPS 700.100; and Inspector General Investigative Records, USPS 700.300*, are exempt from subsections 552a(c)(3), (d)(1)–(4), (e)(1), (e)(4) (G) and (H), and (f) for the same reasons as stated in paragraph (b)(2) of this section.

(ii) *Labor Relations Records, USPS 200.000*, is exempt from subsections 552a(d)(1)–(4), (e)(4)(G) and (H), and (f) for the following reasons:

(A) Application of the requirements at subsections (d)(1)–(4) would cause disruption of enforcement of the laws relating to equal employment opportunity (EEO). It is essential to the integrity of the EEO complaint system that information collected in the investigative process not be prematurely disclosed and that witnesses be free from restraint, interference, coercion, or reprisal.

(B) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply for the same reasons described in paragraph (b)(2)(iv) of this section.

(iii) *Financial Transactions, USPS 860.000*, is exempt from subsections 552a(c)(3), (d)(1)–(4), (e)(1), (e)(4)(G) and (H), and (f) for the following reasons:

(A) Disclosure to the record subject pursuant to subsections (c)(3) and (d)(1)–(4) would violate the non-notification provision of the Bank Secrecy Act, 31 U.S.C. 5318(g)(2), under which the Postal Service is prohibited from notifying a transaction participant that a suspicious transaction report has been made. In addition, the access provisions of subsections (c)(3) and (d)(1)–(4) would alert individuals that they have been identified as suspects or possible subjects of investigation and thus seriously hinder the law enforcement purposes underlying the suspicious transaction reports.

(B) This system is in compliance with subsection (e)(1) because maintenance of the records is required by law. Strict application of the relevance and necessity requirements of subsection (e)(1)

to suspicious transactions would be impractical, however, because the relevance or necessity of specific information can often be established only after considerable analysis and as an investigation progresses.

(C) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply because this system is exempt from the provisions of subsection (d). Nevertheless, the Postal Service has published notice of its notification, access, and contest procedures because access is appropriate in some cases.

(4) Pursuant to subsection 552a(k)(5), *Recruiting, Examining, and Placement Records, USPS 100.100; Labor Relations Records, USPS 200.000; Inspection Service Investigative File System, USPS 700.000; and Inspector General Investigative Records, USPS 700.300* are exempt from certain subsections of 5 U.S.C. 552a because the systems contain investigatory material compiled for the purpose of determining suitability, eligibility, or qualifications for employment, contracts, or access to classified information.

(i) *Recruiting, Examining, and Placement Records, USPS 100.100*, is exempt from subsections 552a(d)(1)–(4) and (e)(1) for the following reasons:

(A) During its investigation and evaluation of an applicant for a position, the Postal Service contacts individuals who, without an assurance of anonymity, would refuse to provide information concerning the subject of the investigation. If a record subject were given access pursuant to subsection (d)(1)–(4), the promised confidentiality would be breached and the confidential source would be identified. The result would be restriction of the free flow of information vital to a determination of an individual's qualifications and suitability for appointment to or continued occupancy of his or her position.

(B) In collecting information for investigative and evaluative purposes, it is impossible to determine in advance what information might be of assistance in determining the qualifications and suitability of an individual for appointment. Information that seems irrelevant, when linked with other information, can sometimes provide a composite picture of an individual that assists in determining whether that indi-

vidual should be appointed to or retained in a position. For this reason, exemption from subsection (e)(1) is claimed.

(C) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply because this system is exempt from the provisions of subsection (d). Nevertheless, the Postal Service has published notice of its notification, access, and contest procedures because access is appropriate in some cases.

(ii) *Labor Relations Records, USPS 200.000*, is exempt from subsections 552a(d)(1)–(4), (e)(4)(G) and (H), and (f) for the following reasons:

(A) Application of the provisions at subsection (d)(1)–(4) would reveal to the EEO complainant the identity of individuals who supplied information under a promise of anonymity. It is essential to the integrity of the EEO complaint system that information collected in the investigative process not be prematurely disclosed and that witnesses be free from restraint, interference, coercion, or reprisal.

(B) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply because this system is exempt from the provisions of subsection (d). Nevertheless, the Postal Service has published notice of its notification, access, and contest procedures because access is appropriate in some cases.

(iii) *Inspection Service Investigative File System, USPS 700.000; and Inspector General Investigative Records, USPS 700.300*, are exempt from subsections 552a(c)(3), (d)(1)–(4), (e)(1), (e)(4)(G) and (H), and (f) for the same reasons as stated in paragraph (b)(2) of this section.

(5) Pursuant to subsection 552a(k)(6), *Employee Development and Training Records, USPS 100.300; Personnel Research Records, 100.600; and Emergency Management Records, USPS 500.300* are exempt from subsections 552a(d)(1)–(4), (e)(4)(G) and (H), and (f) because the systems contain testing or examination material the disclosure of which would compromise the objectivity or fairness of the material. The reasons for exemption follow:

(i) These systems contain questions and answers to standard testing materials, the disclosure of which would compromise the fairness of the future

§ 266.10

39 CFR Ch. I (7–1–13 Edition)

use of these materials. It is not feasible to develop entirely new examinations after each administration as would be necessary if questions or answers were available for inspection and copying. Consequently, exemption from subsection (d) is claimed.

(ii) The requirements of subsections (e)(4)(G) and (H), and (f) do not apply because this system is exempt from the provisions of subsection (d). Nevertheless, the Postal Service has published notice of its notification, access, and contest procedures because access is appropriate in some cases.

[70 FR 22513, Apr. 29, 2005]

§ 266.10 Computer matching.

(a) *General.* Any agency or Postal Service component that wishes to use records from a Postal Service automated system of records in a computerized comparison with other postal or non-postal records must submit its proposal to the Postal Service Manager Records Office. Computer matching programs as defined in paragraph (c) of § 262.5 must be conducted in accordance with the Privacy Act, implementing guidance issued by the Office of Management and Budget and these regulations. Records may not be exchanged for a matching program until all procedural requirements of the Act and these regulations have been met. Other matching activities must be conducted in accordance with the Privacy Act and with the approval of the Manager, Records Office. See paragraph (b)(6) of § 266.4.

(b) *Procedure for submission of matching proposals.* A proposal must include information required for the matching agreement discussed in paragraph (d)(1) of this section. The Inspection Service must submit its proposals for matching programs and other matching activities to the Postal Service Manager Records Office through: Independent Counsel, Inspection Service, U.S. Postal Service, 475 L'Enfant Plaza SW, Rm 3417, Washington, DC 20260–2181. All other matching proposals, whether from postal organizations or other government agencies, must be mailed directly to: Manager, Records Office, U.S. Postal Service, 475 L'Enfant Plaza SW., Washington, DC 20260.

(c) *Lead time.* Proposals must be submitted to the Postal Service Manager Records Office at least 3 months in advance of the anticipated starting date to allow time to meet Privacy Act publication and review requirements.

(d) *Matching agreements.* The participants in a computer matching program must enter into a written agreement specifying the terms under which the matching program is to be conducted. The Manager, Records Office may require similar written agreements for other matching activities.

(1) *Content.* Agreements must specify:

(i) The purpose and legal authority for conducting the matching program;

(ii) The justification for the program and the anticipated results, including, when appropriate, a specific estimate of any savings in terms of expected costs and benefits, in sufficient detail for the Data Integrity Board to make an informed decision;

(iii) A description of the records that are to be matched, including the data elements to be used, the number of records, and the approximate dates of the matching program;

(iv) Procedures for providing notice to individuals who supply information that the information may be subject to verification through computer matching programs;

(v) Procedures for verifying information produced in a matching program and for providing individuals an opportunity to contest the findings in accordance with the requirement that an agency may not take adverse action against an individual as a result of information produced by a matching program until the agency has independently verified the information and provided the individual with due process;

(vi) Procedures for ensuring the administrative, technical, and physical security of the records matched; for the retention and timely destruction of records created by the matching program; and for the use and return or destruction of records used in the program;

(vii) Prohibitions concerning duplication and redisclosure of records exchanged, except where required by law or essential to the conduct of the matching program;

(viii) Assessments of the accuracy of the records to be used in the matching program; and

(ix) A statement that the Comptroller General may have access to all records of the participant agencies in order to monitor compliance with the agreement.

(2) *Approval.* Before the Postal Service may participate in a computer matching program or other computer matching activity that involves both USPS and non-USPS records, the Data Integrity Board must have evaluated the proposed match and approved the terms of the matching agreement. To be effective, the matching agreement must receive approval by each member of the Board. Votes are collected by the Postal Service Manager Records Office. Agreements are signed on behalf of the Board by the Chairman. If a matching agreement is disapproved by the Board, any party may appeal the disapproval in writing to the Director, Office of Management and Budget, Washington, DC 20503-0001, within 30 days following the Board's written disapproval.

(3) *Effective dates.* No matching agreement is effective until 40 days after the date on which a copy is sent to Congress. The agreement remains in effect only as long as necessary to accomplish the specific matching purpose, but no longer than 18 months, at which time the agreement expires unless extended. The Data Integrity Board may extend an agreement for one additional year, without further review, if within 3 months prior to expiration of the 18-month period it finds that the matching program is to be conducted without change, and each party to the agreement certifies that the program has been conducted in compliance with the matching agreement. Renewal of a continuing matching program that has run for the full 30-month period requires a new agreement that has received Data Integrity Board approval.

[59 FR 37161, July 21, 1994, as amended at 60 FR 57345, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003; 69 FR 34935, June 23, 2004]

PART 267—PROTECTION OF INFORMATION

Sec.

267.1 Purpose and scope.

267.2 Policy.

267.3 Responsibility.

267.4 Information security standards.

267.5 National Security Information.

AUTHORITY: 39 U.S.C. 401; Pub. L. 93-579, 88 Stat. 1896.

§ 267.1 Purpose and scope.

This part addresses the protection of information and records in the custody of the Postal Service throughout all phases of information flow and within all organization components, and includes micromated, manual and data processing information.

[40 FR 45726, Oct. 2, 1975]

§ 267.2 Policy.

Consistent with the responsibility of the Postal Service to make its official records available to the public to the maximum extent required by the public interest, and to ensure the security, confidentiality, and integrity of official records containing sensitive or national security information, it is the policy of the Postal Service to maintain definitive and uniform information security safeguards. These safeguards will have as their purpose: (a) Ensuring the effective operation of the Postal Service through appropriate controls over critical information, and (b) Protecting personal privacy, the public interest, and the national security by limiting unauthorized access to both restricted and national security information.

[44 FR 51224, Aug. 31, 1979]

§ 267.3 Responsibility.

(a) *Chief Postal Inspector and Chief Privacy Officer.* The Chief Postal Inspector and the Chief Privacy Officer will ensure within their respective areas of jurisdiction:

(1) Postal Service-wide compliance with this policy and related standards and procedures; and

(2) Implementation of remedial action when violations or attempted violations of these standards and procedures occur.