



7710-12

POSTAL SERVICE

39 CFR Part 266

Privacy of Information

AGENCY: Postal Service™.

ACTION: Final rule.

SUMMARY: The Postal Service is revising and restating its privacy regulations to implement numerous non-substantive editorial changes. These include renaming certain offices with privacy-related duties, modification of the roles of employees tasked with implementing aspects of the privacy regulations, and minor editorial changes to postal privacy policy to improve its consistency and clarity. These rules contain procedures by which individuals may request notification of and access to records about themselves, request amendments to those records, or request an accounting of disclosures of those records by the Postal Service.

DATES: Effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Natalie A. Bonanno, Chief Counsel, Federal Compliance, natalie.a.bonanno@usps.gov, 202-268-2944.

SUPPLEMENTARY INFORMATION: As revised and restated, 39 CFR part 266 is designed to carry forward the substantive content of former §§ 266.1 – 266.10 in an updated, accessible format.

266.1 Purpose and scope:

The Postal Service has revised § 266.1 to align with the purpose and scope of the Privacy Act of 1974, which provides the authority for these regulations. (The Postal

Service has deleted former § 266.2 *Policy* because it did not add any significant provisions, instructions, or guidance to these regulations, and has redesignated former §§ 266.3 – 266.10 as §§ 266.2 – 266.9, respectively.)

266.2 Responsibility:

In revised § 266.2 and throughout these regulations, the Postal Service has updated office names to reflect its current administrative structure. Thus, “Records Office” has been changed to “Privacy and Records Management Office” to reflect the new name of this office. Similarly, “Custodian” has been changed to “Records Custodian” for clarity, and the “Information System Executive” has become the “Corporate Information Security Office” to reflect the new name and role of this functional organization.

Similarly, in revised § 266.2 and throughout these regulations, the Postal Service has revised the titles of certain employees to reflect their new titles. Specifically, “Chief Privacy Officer” was changed to “Chief Privacy and Records Management Officer,” “Senior Vice President, Human Resources” was changed to “Chief Human Resources Officer and Executive Vice President” and “Vice President, General Counsel” was changed to “General Counsel and Executive Vice President.”

266.3 Collection and disclosure of information about individuals:

In revised § 266.3(b)(3), the Postal Service has defined the limited circumstances in which a mailing list may be disclosed. The Postal Service has also replaced the word “correction” with “amendment” in this section and throughout these regulations.

266.4 Notification:

No substantive changes have been made to revised § 266.4. Minor editorial changes have been made to ensure clarity and consistency of format.

266.5 Procedures for requesting notification, inspection, copying, or amendment of records:

In revised § 266.5(b)(2), the Postal Service has added a list of the acceptable identity verification methods that a requester may use to satisfy a records custodian as to the requester's identity before review or other access to a record containing personal information is granted. The Postal Service has also added a new paragraph 266.5(c) entitled *Compliance with notification request* to ensure custodians understand their responsibilities and requesters are aware of their rights in this regard.

266.6 Appeal procedure:

In revised § 266.6(a)(2), the Postal Service has extended the period in which a requester may file an appeal from 30 days to 90 days.

266.7 Schedule of fees; 266.8 Exemptions; and 266.9 Computer matching:

No substantive changes have been made to revised §§ 266.7 – 266.9. Minor editorial changes have been made to ensure clarity and consistency of format.

List of Subjects in 39 CFR Part 266

Privacy.

For the reasons stated in the preamble, the Postal Service amends 39 CFR chapter I by revising part 266 to read as follows:

PART 266—PRIVACY OF INFORMATION

Sec.

266.1 Purpose and scope.

266.2 Responsibility.

266.3 Collection and disclosure of information about individuals.

266.4 Notification.

266.5 Procedures for requesting inspection, copying, or amendment of records.

266.6 Appeal procedure.

266.7 Schedule of fees.

266.8 Exemptions.

266.9 Computer matching.

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

§ 266.1 Purpose and scope.

This part contains the rules that the Postal Service follows under the Privacy Act of 1974, 5 U.S.C. 552a. These rules should be read together with the Privacy Act, which provides additional information about records maintained on individuals. The rules in this part apply to all records in systems of records maintained by the Postal Service that are retrieved by an individual's name or personal identifier. They describe the procedures by which individuals may request notification of or access to records about themselves, request amendment of those records, and request an accounting of disclosures of those records by the Postal Service. In addition, the Postal Service processes all Privacy Act requests for access to records under the Freedom of Information Act (FOIA), 5 U.S.C. 552, following the rules contained in 39 CFR 265, as necessary, which provides the requester with the greatest access to his or her personal records.

§ 266.2 Responsibility.

(a) *Privacy and Records Management Office.* The Privacy and Records Management Office will ensure Postal Service-wide compliance with this part.

(b) *Records Custodian*. Records Custodians are responsible for adherence to this part within their respective units, and in particular for affording individuals their rights to inspect and obtain copies of records concerning them.

(c) *Corporate Information Security Office*. This office is responsible for ensuring compliance with information security policies, including protection of information resources containing customer, employee, or other individuals' information; developing policy for safeguarding and disposing of electronic records (including emails) that are maintained in information systems (including those that are subject to legal holds); serving as the central contact for information security issues; preventing and engaging in some investigation of cybercrime and misuse of Postal Service information technology resources; and providing security consultation as requested.

(d) *Data Integrity Board—(1) Responsibilities*. The Data Integrity Board oversees Postal Service computer matching activities. The Board's 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 advice functions relating to record 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 and Records Management 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) General Counsel and Executive Vice President (Chairman).
- (ii) Chief Postal Inspector.
- (iii) Inspector General.
- (iv) Chief Human Resources Officer and Executive Vice President.
- (v) Chief Privacy and Records Management Officer.

§ 266.3 Collection and disclosure of information about individuals.

(a) This section governs the collection of information about individuals, as defined in the Privacy Act of 1974, 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 authorized 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 individuals who have been asked to furnish information about themselves, 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 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 disfavor any individual who fails or refuses to provide personal information 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 an individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the information is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

(4) The Postal Service will not require an individual to furnish a Social Security number or deny a right, privilege or benefit because of that individual's refusal to furnish the number unless required by Federal law.

(b) *Disclosures—(1) Limitations.* 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 to the extent provided by the Privacy Act and unless:

(i) The individual to whom the record pertains has requested in writing that the information be disseminated, unless the individual would not be entitled to access to the record under the Postal Reorganization Act, the Privacy Act, or other law;

(ii) The requester has obtained the prior written consent of the individual to whom the record pertains, unless the individual would not be entitled to access to the record under the Postal Reorganization Act, the Privacy Act, or other law; or

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

(2) *Dissemination.* 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 or employees of a Postal Service contractor who have a need for such information in the performance of their Postal Service 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 of the U.S. Code;

(vi) To the National Archives and Records Administration 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 Archivist of the United States or an authorized 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 that officer's authorized representatives in the course of the performance of the duties of the Government Accountability Office; or

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

(3) Under 39 U.S.C. 412(a), the Postal Service may make a mailing or other list of names and addresses of past or present postal patrons or other persons available to the public only to the extent that such action is authorized by law. Consistent with this provision, the Postal Service may make such a list available as follows:

(i) In accordance with 39 U.S.C. 412(b), to the Secretary of Commerce for use by the Bureau of the Census;

(ii) As required by the terms of a legally enforceable contract entered into by the Postal Service under its authority contained in 39 U.S.C. 401(3) and when subject to a valid non-disclosure agreement;

(iii) As required by the terms of a legally enforceable interagency agreement entered into by the Postal Service under its authority contained in 39 U.S.C. 411 and when subject to a valid non-disclosure agreement;

(iv) In accordance with 5 U.S.C. 552a(b), the Postal Service may disclose a list of names and addresses of individuals pursuant to a written request by, or with the prior written consent of, each individual whose name and address is contained in such list, provided that such names and addresses are derived from records maintained by the Postal Service in a system of records as defined by 5 U.S.C. 552a(a); or

(v) As otherwise expressly authorized by federal law.

(4) *Employee credit references.* A credit bureau or other commercial firm from which a current or former postal employee is seeking credit may be given the following past or present information upon request: grade, duty station, dates of employment, job title, and salary. If additional information is desired, the requester must submit the written consent of the employee and an accounting of the disclosure must be kept.

(5) *Employee job references.* Upon request, prospective employers of a current or 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 § 262.5(c) and (d), 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 Chief Privacy and Records Management Officer determines the applicability of a particular routine use and the necessity for adoption of a new routine use.

(ii) *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 § 266.9). The Privacy and Records Management Office may require that other matching activities be conducted in accordance with a written agreement.

(iii) *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 § 266.9). Other matching activities may, at the discretion of the Privacy and Records Management Office, be submitted for Board approval.

(c) *Amendment or dispute disclosure.* If a personal record contains any amendments or notations of dispute relating to the accuracy, timeliness or relevance of the record, any person or other agency to which the record has been or is to be disclosed must be informed of the amendments or notations within 30 days of the modification.

(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, to Postal Service employees or employees of Postal Service contractors in the performance of their Postal Service duties, when the record is publicly available, or as required by the Freedom of Information Act (5 U.S.C. 552).

(2) The accounting will be maintained for at least 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 paragraph (b)(2)(viii) of this section relating to law enforcement activities.

§ 266.4 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 that individual, unless exempt from notification under the Privacy Act or other law. See § 266.5 for the suggested form of a request.

(b) *Notification of disclosure.* The Postal Service will 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 § 266.5(c)(1) relating to amendment of records upon request.

(d) *Notification of new use.* Any new intended use of personal information maintained by the Postal Service will be published in the *Federal Register* 30 days before such use becomes operational. Public views may then be submitted to the Privacy and Records Management Office.

(e) *Notification of exemptions.* The Postal Service will publish in the *Federal Register* its intent to exempt any system of records and will 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 to the Office of Management and Budget (OMB) 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, and published at least 30 days prior to:

(1) The initiation of any matching activity under a new or substantially revised program; or

(2) The expiration of the existing matching agreement in the case of a renewal of a continuing program.

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

The purpose of this section is to provide procedures by which an individual may request notification of, access to, or amendment of 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 in accordance with the procedures described in the applicable

system of records notice, or to the Privacy and Records Management Office, U.S. Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101. Requests to the U.S. Postal Inspection Service should be submitted to the Chief Postal Inspector, U.S. Postal Inspection Service, 475 L'Enfant Plaza SW, Washington, DC 20260. Requests to the Office of Inspector General should be submitted to the Freedom of Information Act/Privacy Officer, U.S. Postal Service Office of Inspector General, 1735 North Lynn Street, Arlington, VA 22209-2020. Inquiries should be clearly marked, "Privacy Act Request." Any inquiry concerning a specific system of records should include the information contained under "Notification Procedure" for that system as published in the *Federal Register* or within USPS Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management, Appendix*. If the information supplied is insufficient to locate or identify the record, if any, the requester will be notified promptly and, if possible, informed of additional information required. Amendment requests that contest the relevance, accuracy, timeliness or completeness of the record should include a statement of the amendment requested.

(2) *Period for response by custodian.* Upon receipt of an inquiry, the custodian will respond with an acknowledgement of receipt within 10 days.

(b) *Compliance with request for access—(1) Notification to requester.* When a requested record has been identified and is to be made available to the requester for inspection and copying, the custodian must ensure that the record is made available promptly and must immediately notify the requester where and when the record will be available for inspection and 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 that are in the custodian's possession. If the requested record has been identified and a copy is to be provided to the requester, the copy must be promptly provided.

(2) *Identification of requester.* The requester must present identification sufficient to satisfy the custodian as to the requester's identity prior to record review or other access. As appropriate under the circumstances of the access request, the requester may be required to comply with one of the following identification verification methods:

(i) Provision of a completed *Certification of Identity* if the records pertain to the requester available at <http://about.usps.com/who-we-are/foia/welcome.htm>;

(ii) Provision of official photo identification if the records pertain to the requester, examples of which are a valid driver's license, unexpired passport, and unexpired federal government-issued employee identification card; or

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

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

(i) The requester must agree not to leave Postal Service premises with official records unless specifically given a copy for that purpose by the custodian or the custodian's representative.

(ii) At the conclusion of the inspection, the requester must sign a statement indicating the requester has reviewed specific records or categories of records. If the requester indicates at the beginning of the inspection that he or she will not sign the

statement, records may still be reviewed, and the time and date of review will be noted in the file.

(iii) The requester may be accompanied by a person of the requester's choice to aid in the inspection of information and, if applicable, the manual recording or copying of the records if the requester submits a signed statement authorizing the person to do so, and discussion of the records in the accompanying person's presence.

(4) *Special restrictions for medical and psychological records.* A medical or psychological record must 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 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. In such cases, an accounting of the disclosure must be kept.

(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 specifically addressed in paragraph (b)(4) of this section and § 266.8.

(6) *Response when compliance is not possible.* A reply denying a written request to review or otherwise access a record must be in writing, signed by the custodian or other appropriate official and must 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 must include a statement regarding the determining factors of denial, and the right to appeal the denial to the General Counsel.

(c) *Compliance with notification request.* The custodian must promptly notify a requester if a record has been located in response to a request for notification as to whether a specific system of records contains a record pertaining to the requester, unless exempt from notification.

(d) *Compliance with request for amendment.* The custodian must:

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

(e) *Availability of assistance in exercising rights.* The Privacy and Records Management Office is available to provide an individual with assistance in exercising rights pursuant to this part.

§ 266.6 Appeal procedure.

(a) *Appeal procedure.* (1) If a request for notification of or to inspect, copy, or amend a record is denied, in whole or in part, or if no determination is made within the period prescribed by this part, the requester may appeal to the General Counsel, U.S. Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101.

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

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

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

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

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

(4) The decision of the General Counsel constitutes the final decision of the Postal Service on the right of the requester to be notified of; inspect, copy, or otherwise have access to; or change or update a record. The decision on the appeal must be in writing and, in the event of a denial, must 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 must 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.

§ 266.7 Schedule of fees.

(a) *Policy.* The purpose of this section is to establish fair and equitable fees to 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 must be furnished without charge. See paragraph (c) of this section for fee limitations.

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

(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; a fee of \$0.15 per page is charged for each copy of each duplicate page without regard to whether the requester is eligible for free copies pursuant to § 266.7(b)(1).

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

(d) *Reimbursement.* 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 set forth at § 265.9.

§ 266.8 Exemptions.

(a) The Postal Reorganization Act, 39 U.S.C. 410(c), provides that certain categories of information are exempt from disclosure under the Privacy Act. In addition, the Privacy Act, 5 U.S.C. 552a(j) and (k), authorizes 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 summarizes the 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, 5 U.S.C. 552a(j) and (k). 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 of 5 U.S.C. 552a for which an exemption is claimed in the systems discussed in this section.* (i) Subsection (c)(3) of 5 U.S.C. 552a requires an agency to make available to the individual named in the records an accounting of each disclosure of records at the individual's request.

(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) Subsections (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 (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 apply the requirements of 5 U.S.C. 552a to a contractor operating a system of records to accomplish an agency function.

(2) Pursuant to 5 U.S.C. 552a(j)(2), Postal Service record systems; *Inspection Service Investigative File System, USPS 700.000; Mail Cover Program Records, USPS 700.100; Inspector General Investigative Records, USPS 700.300* are exempt from subsections 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 make them 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; or

(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 (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 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 (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 these systems are 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 will remain applicable to it (subsection (m)).

(3) Pursuant to 5 U.S.C. 552a(k)(2), Postal Service record systems *Labor Relations Records, USPS 200.000; Employee Inquiry, Complaint and Investigative Records, USPS 100.900; 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) *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 the 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.

(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 of 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 5 U.S.C. 552a(k)(5), Postal Service record systems *Recruiting, Examining, and Placement Records, USPS 100.100; 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 individual 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) *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 5 U.S.C. 552a(k)(6), Postal Service record systems *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 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 these systems are 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.

§ 266.9 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 Privacy and Records Management Office. Computer matching programs as defined in §

262.5(c) must be conducted in accordance with the Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988. 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 Privacy and Records Management Office. See § 266.3(b)(6).

(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 Privacy and Records Management Office through: Counsel, Inspection Service, U.S. Postal Service, 475 L'Enfant Plaza, SW, Washington, DC 20260. All other matching proposals, whether from postal organizations or other government agencies, must be mailed directly to: Privacy and Records Management Office, U.S. Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1101.

(c) *Lead time.* Proposals must be submitted to the Postal Service Privacy and Records Management Office at least three 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 Privacy and Records Management 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 unanimously approved the terms of the matching agreement. Agreements are executed by the Chairman of the Board. 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, within 30 days following the Board's written disapproval.

(3) *Effective dates.* The agreement will become effective in accordance with the date in the matching agreement and as provided to Congress and the Office of Management and Budget and published in the *Federal Register*. 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 three 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.

Stanley F. Mires,

Attorney, Federal Compliance.

[FR Doc. 2017-21850 Filed: 10/10/2017 8:45 am; Publication Date: 10/11/2017]