§ 267.4 Information security standards.

(a) The Postal Service will operate under a uniform set of information security standards which address the following functional aspects of information flow and management:

(1) Information system development,

(2) Information collection,

(3) Information handling and processing,

(4) Information dissemination and disclosure,

(5) Information storage and destruction,

(b) Supplementing this list are information security standards pertaining to the following administrative areas:

(1) Personnel selection and training,

(2) Physical environment protection,

(3) Contingency planning,

(4) Information processing or storage system procurement,

(5) Contractual relationships.

[40 FR 45726, Oct. 2, 1975; 40 FR 48512, Oct. 16, 1975]

§ 267.5 National Security Information.

(a) *Purpose and scope.* The purpose of this section is to provide regulations implementing Executive Order 12356 National Security Information (hereinafter referred to as the Executive Order) which deals with the protection, handling and classification of national security information.

(b) *Definitions.* (1) In this section, *National Security Information* means information on the national defense and foreign relations of the United States that has been determined under the Executive Order or prior Orders to require protection against unauthorized disclosure and has been so designated.

(2) *Derivative Classification* means the carrying forward of a classification from one document to a newly created document that contains national security information which is in substance the same as information that is currently classified.

(3) *In the Custody of the Postal Service* means any national security information transmitted to and held by the U.S. Postal Service for the information and use of postal officials. (This does not include any national security information in the U.S. Mails.)

(c) *Responsibility and authority.* (1) The Manager, Payroll Accounting and Records, serves as the USPS National Security Information Oversight Officer. This officer shall:

(i) Conduct an active oversight program to ensure that the appropriate provisions of these regulations are complied with;

(ii) Chair a committee composed of the Manager, Payroll Accounting and Records; the Chief Postal Inspector (USPS Security Officer); the General Counsel; the Executive Assistant to the Postmaster General; and the Director, Operating Policies Office; or their designees, with authority to act on all suggestions and complaints concerning compliance by the Postal Service with the regulations in this part;

(iii) Ensure that appropriate and prompt corrective action is taken whenever a postal employee knowingly, willfully and without authorization:

(A) Discloses national security information properly classified under the Executive order, or prior orders,

(B) Compromises properly classified information through negligence, or

(C) Violates any provisions of these regulations or procedures;

(iv) Establish, staff, and direct activities for controlling documents containing national security information at USPS Headquarters and to provide functional direction to the field.

(v) In conjunction with the USPS Security Officer, prepare and issue instructions for the control, protection, and derivative classification of national security information in the custody of, and use by, the Postal Service. These instructions shall include requirements that:

(A) A demonstrable need for access to national security information is established before requesting the initiation of administrative clearance procedures;

(B) Ensure that the number of people granted access to national security information is reduced to and maintained at the minimum number consistent with operational requirements and needs;

(vi) Establish, staff and direct activities for controlling documents containing national security information at USPS Headquarters and provide

functional direction to each Regional Records Control Officer;

(vii) As part of the overall program implementation, develop a training program to familiarize appropriate postal employees of the requirements for control, protection and classification; and

(viii) Report to the USPS Security Officer any incidents of possible loss or compromise of national security information.

(2) The USPS Security Officer (the Chief Postal Inspector) shall:

(i) Provide technical guidance to the Manager, Payroll Accounting and Records in implementing the national security information program;

(ii) Conduct investigations into reported program violations or loss or possible compromise of national security information and report any actual loss or compromise to the originating agency;

(iii) Periodically conduct an audit of the USPS national security information program;

(iv) Process requests for sensitive clearances; conduct the appropriate investigations and grant or deny a sensitive clearance to postal employees having an official ''need to know'' national security information; and

(v) Report to the Attorney General any evidence of possible violations of federal criminal law by a USPS employee and of possible violations by any other person of those federal criminal laws.

(3) All postal employees who have access to national security information shall:

(i) Sign a nondisclosure agreement;

(ii) Be familiar with and follow all Program regulations and instructions;

(iii) Actively protect and be accountable for all national security information entrusted to their care;

(iv) Disclose national security information only to another individual who is authorized access;

(v) Immediately report to the Manager, Payroll Accounting and Records and the USPS Security Officer any suspected or actual loss or compromise of national security information; and

(vi) Be subject to administrative sanctions should requirements (ii) through (v) not be followed.

(d) *Derivative classification*. When applying derivative classifications to documents created by the Postal Service, the Postal Service shall:

(1) Respect original classification decisions;

(2) Verify the information's current level of classification so far as practicable before applying the markings; and

(3) Carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings in accordance with section 2 of the Executive order.

(e) *General provisions*—(1) *Dissemination*. National security information received by the U.S. Postal Service shall not be further disseminated to any other agency without the consent of the originating agency.

(2) *Disposal*. Classified documents no longer needed by the Postal Service shall be either properly destroyed or returned to the originating agency.

(3) Freedom of Information Act or mandatory review requests.

(i) Requests for classified documents made under the Freedom of Information Act (FOIA) and mandatory review requests (requests under Section 3–501 of the Executive Order for the declassification and release of information), including requests by the news media, should be submitted to: Manager, Records Office, U.S. Postal Service, 475 L'Enfant Plaza, SW., Washington, DC 20260.

(ii) In response to an FOIA request or a mandatory review request, the Postal Service shall not refuse to confirm the existence or non-existence of a document, unless the fact of its existence or non-existence would itself be classifiable.

(iii) The Postal Service shall forward all FOIA and mandatory review requests for national security information in its custody (including that within records derivatively classified by the USPS) to the originating agency for review unless the agency objects on the grounds that its association with the information requires protection. The requester shall be notified that:

(A) The request was referred; and

(B) The originating agency will provide a direct response.

(4) *Research requests.* Requests from historical researchers for access to national security information shall be referred to the originating agency.

(39 U.S.C. 401 (2), (10), 404(a)(7))

[44 FR 51224, Aug. 31, 1979, as amended at 45 FR 30069, May 7, 1980; 49 FR 22476, May 30, 1984; 60 FR 57345, 57346, Nov. 15, 1995; 64 FR 41291, July 30, 1999; 68 FR 56560, Oct. 1, 2003]

PART 268—PRIVACY OF INFORMATION—EMPLOYEE RULES OF CONDUCT

Sec.
268.1 General principles.
268.2 Consequences of non-compliance.

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

§ 268.1 General principles.

In order to conduct its business, the Postal Service has the need to collect various types of personally identifiable information about its customers, employees and other individuals. Information of this nature has been entrusted to the Postal Service, and employees handling it have a legal and ethical obligation to hold it in confidence and to actively protect it from uses other than those compatible with the purpose for which the information was collected. This obligation is legally imposed by the Privacy Act of 1974, which places specific requirements upon all Federal agencies, including the Postal Service, and their employees. In implementation of these requirements, the following rules of conduct apply:

(a) Except as specifically authorized in §266.4(b)(2) of this chapter, no employee shall disclose, directly or indirectly, the contents of any record about another individual to any person or organization. Managers are to provide guidance in this regard to all employees who must handle such information.

(b) *No employee will maintain a secret system of records about individuals.* All records systems containing personally identifiable information about individuals must be reported to the Manager, Records Office.

(c) All employees shall adhere strictly to the procedures established by the U.S. Postal Service to ensure the confidentiality and integrity of information about individuals that is collected, maintained and used for official Postal Service business. Employees shall be held responsible for any violation of these procedures.

[45 FR 44273, July 1, 1980, as amended at 60 FR 57346, Nov. 15, 1995; 68 FR 56560, Oct. 1, 2003]

§ 268.2 Consequences of non-compliance.

(a) The Privacy Act authorizes any individual, whether or not an employee, to bring a civil action in U.S. District Court to obtain judicial review of the failure of the Postal Service to comply with the requirements of the Act or its implementing regulations. In certain instances of willful or intentional non-compliance, the plaintiff may recover damages from the Postal Service in the minimum amount of $1,000 together with costs of the action and attorney fees.

(b) The Act provides criminal sanctions for individuals, including employees, who violate certain of its provisions.

(1) Any officer or employee who, by virtue of his employment or position, has possession of, or access to, official records which contain individually identifiable information and who, knowing that disclosure of the specific material is prohibited by Postal Service regulations, willfully discloses the material to a person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee who willfully maintains a system of records without meeting the notice requirements set forth in Postal Service regulations shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning another individual from the Postal Service under false pretense shall be guilty of a misdemeanor and fined not more than $5,000.

(c) In addition to the criminal sanctions, any employee violating any provisions of these rules of conduct is subject to disciplinary action which may