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.

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 result in dismissal from the Postal Service.

[40 FR 45726, Oct. 2, 1975]

PART 273—ADMINISTRATION OF PROGRAM FRAUD CIVIL REMEDIES ACT

Sec.

AUTHORITY: 31 U.S.C. Chapter 38; 39 U.S.C. 401.