

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.

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.

(b) *Custodians.* All custodians are responsible for insuring that information security standards and procedures are followed and that all relevant employees participate in the information security awareness programs.

[40 FR 45726, Oct. 2, 1975, as amended at 60 FR 57345, Nov. 15, 1995; 68 FR 56560, Oct. 1, 2003]

§ 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,

§ 267.5

(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 know-

39 CFR Ch. I (7-1-20 Edition)

ingly, 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