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.

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,