§ 266.10 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 Manager Records Office. Computer matching programs as defined in paragraph (c) of §262.5 must be conducted in accordance with the Privacy Act, implementing guidance issued by the Office of Management and Budget and these regulations. 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 Manager, Records Office. See paragraph (b)(6) of §266.4.

(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 Postal Service Manager Records Office through: Independent Counsel, Inspection Service, U.S. Postal Service, 475 L’Enfant Plaza SW, Rm 3417, Washington, DC 20260-2181. All other matching proposals, whether from postal organizations or other government agencies, must be mailed directly to: Manager, Records Office, U.S. Postal Service, 475 L’Enfant Plaza SW, Washington, DC 20260.

(c) Lead time. Proposals must be submitted to the Postal Service Manager Records Office at least 3 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 Manager, Records Office may require similar written agreements for other matching activities.

(i) 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 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;

(v) 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;

(vi) Prohibitions concerning duplication and redisclosure of records exchanged, except where required by law or essential to the conduct of the matching program;

(vii) 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 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 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.

[70 FR 22513, Apr. 29, 2005]
records of the participant agencies in order to monitor compliance with the
agreement.

(2) Approval. Before the Postal Serv-
ice 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 approved the
terms of the matching agreement. To
be effective, the matching agreement
must receive approval by each member
of the Board. Votes are collected by the
Postal Service Manager Records Office.
Agreements are signed on behalf of the
Board by the Chairman. 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 20503–0001, within 30 days following
the Board’s written disapproval.

(3) Effective dates. No matching agree-
ment is effective until 40 days after the
date on which a copy is sent to Con-
gress. The agreement remains in effect
only as long as necessary to accom-
plish the specific matching purpose,
but no longer than 18 months, at which
time the agreement expires unless ex-
tended. The Data Integrity Board may
extend an agreement for one additional
year, without further review, if within
3 months prior to expiration of the 18-
month period it finds that the match-
ing program is to be conducted without
change, and each party to the agree-
ment certifies that the program has
been conducted in compliance with the
matching agreement. Renewal of a con-
tinuing matching program that has run
for the full 30-month period requires a
new agreement that has received Data
Integrity Board approval.

[59 FR 37161, July 21, 1994, as amended at 60
FR 57345, Nov. 15, 1995; 64 FR 41291, July 30,
1999; 68 FR 56560, Oct. 1, 2003; 69 FR 34935,
June 23, 2004]

PART 267—PROTECTION OF
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 in-
cludes 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 pub-
lic interest, and to ensure the security,
confidentiality, and integrity of offi-
cial records containing sensitive or na-
tional security information, it is the
policy of the Postal Service to main-
tain definitive and uniform informa-
tion security safeguards. These safe-
guards 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 secu-

[44 FR 51224, Aug. 31, 1979]

§ 267.3 Responsibility.

(a) Chief Postal Inspector and Chief
Privacy Officer. The Chief Postal In-
sector 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 ac-
tion when violations or attempted vio-
lations of these standards and proce-
dures occur.

(b) Custodians. All custodians are re-
sponsible for insuring that information
security standards and procedures are
followed and that all relevant employ-
eses participate in the information se-
curity awareness programs.

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