agency requests for changes in recordkeeping practices governed by the Guide to Personnel Recordkeeping, the Office will examine the proposal or request in the context of such standards set forth by the agency in support of the proposal and in light of the personnel program area that requires these records.

[44 FR 65033, Nov. 9, 1979, as amended at 66 FR 66709, Dec. 27, 2001]

§ 293.104 Collection of information.

(a) Any information in personnel records whether or not those records are in a system of records, used in whole or in part in making a determination about an individual's rights, benefits, or privileges under Federal personnel programs should, to the greatest extent practicable, be collected directly from the individual concerned. Factors to be considered in determining whether to collect the data from the individual concerned or a third party are when:

(1) The nature of the information is such that it can only be obtained from another party;

(2) The cost of collecting the information directly from the individual is unreasonable when compared with the cost of collecting it from another party;

(3) There is virtually no risk that information collected from other parties, if inaccurate, could result in a determination adverse to the individual concerned;

(4) The information supplied by an individual must be verified by another party; or

(5) There are provisions made, to the greatest extent practicable, to vertify information collected from another party with the individual concerned.

§ 293.105 Restrictions on collection and use of information.

(a) First Amendment. Personnel records describing how individuals exercise rights guaranteed by the First Amendment are prohibited unless expressly authorized by statute, or by the individual concerned, or unless pertinent to and within the scope of an authorized law enforcement activity. These rights include, but are not limited to, free exercise of religious and political beliefs, freedom of speech and the press, and freedom to assemble and to petition the government.

(b) Social Security Number.

(1) Agencies may not require individuals to disclose their Social Security Number unless disclosure would be required;

(i) Under Federal statute; or

(ii) Under any statute, Executive order, or regulation that authorizes any Federal, State, or local agency maintaining a system of records that was in existence and operating prior to January 1, 1975, to request the Social Security Number as a necessary means of verifying the identity of an individual.

(2) Individuals asked to voluntarily (circumstances not covered by paragraph (b)(1) of this section) provide their Social Security Number shall suffer no penalty or denial of benefits for refusing to provide it.

§ 293.106 Safeguarding information about individuals.

(a) To ensure the security and confidentiality of personnel records, in whatever form, each agency shall establish administrative, technical, and physical controls to protect information in personnel records from unauthorized access, use, modification, destruction, or disclosure. As a minimum, these controls shall require that all persons whose official duties require access to and use of personnel records be responsible and accountable for safeguarding those records and for ensuring that the records are secured whenever they are not in use or under the direct control of authorized persons. Generally, personnel records should be held, processed, or stored only where facilities and conditions are adequate to prevent unauthorized access.

(b) Personnel records must be stored in metal filing cabinets which are locked when the records are not in use, or in a secured room. Alternative storage facilities may be employed provided they furnish an equivalent or greater degree of security than these methods. Except for access by the data subject, only employees whose official duties require access shall be allowed to handle and use personnel records, in

whatever form or media the records might appear. To the extent feasible, entry into personnel record storage areas shall be similarly limited. Documentation of the removal of records from storage areas must be kept so that adequate control procedures can be established to assure that removed records are returned on a timely basis.

(c) Disposal and destruction of personnel records shall be in accordance with the General Record Schedule issued by the General Services Administration for the records or, alternatively, with Office or agency records control schedules approved by the National Archives and Records Service of the General Services Administration.

§ 293.107 Special safeguards for automated records.

(a) In addition to following the security requirements of § 293.106 of this part, managers of automated personnel records shall establish administrative, technical, physical, and security safeguards for data about individuals in automated records, including input and output documents, reports, punched cards, magnetic tapes, disks, and online computer storage. The safeguards must be in writing to comply with the standards on automated data processing physical security issued by the National Bureau of Standards, U.S. Department of Commerce, and, as a minimum, must be sufficient to:

(1) Prevent careless, accidental, or unintentional disclosure, modification, or destruction of identifiable personal data;

(2) Minimize the risk that skilled technicians or knowledgeable persons could improperly obtain access to, modify, or destroy identifiable personnel data;

(3) Prevent casual entry by unskilled persons who have no official reason for access to such data;

(4) Minimize the risk of an unauthorized disclosure where use is made of identifiable personal data in testing of computer programs;

(5) Control the flow of data into, through, and from agency computer operations;

(6) Adequately protect identifiable data from environmental hazards and unneccessary exposure; and

(7) Assure adequate internal audit procedures to comply with these procedures.

(b) The disposal of identifiable personal data in automated files is to be accomplished in such a manner as to make the data unobtainable to unauthorized personnel. Unneeded personal data stored on reusable media such as magnetic tapes and disks must be erased prior to release of the media for reuse.

§ 293.108 Rules of conduct.

(a) *Scope.* These rules of conduct apply to all Office and agency employees responsible for creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records. The Office and agencies shall require that such employees are familiar with these and appropriate supplemental agency internal regulations.

(b) *Standards of conduct.* Office and agency employees whose official duties involve personnel records shall be sensitive to individual rights to personal privacy and shall not disclose information from any personnel record unless disclosure is part of their official duties or required by executive order, regulation, or statute (e.g., required by the Freedom of Information Act, 5 U.S.C. 552).

(c) *Improper uses of personnel information.* Any Office or agency employee who makes a disclosure of personnel records knowing that such disclosure is unauthorized, or otherwise knowingly violates these regulations, shall be subject to disciplinary action and may also be subject to criminal penalties where the records are subject to the Privacy Act (5 U.S.C. 552a). Employees are prohibited from using personnel information not available to the public, gained through official duties, for commercial solicitation or sale, or for personal gain.