(3) In addition to following the above security requirements, managers of automated personnel records shall establish and maintain 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. As a minimum, the safeguards must be sufficient to:

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

(ii) Minimize the risk of improper access, modification, or destruction of identifiable personnel data;

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

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

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

(vi) Adequately protect identifiable data from environmental hazards and unnecessary exposure; and

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

(4) 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.

(j) At least 30 days prior to publication of information under paragraph (d)(4) of this section, GAO shall publish in the FEDERAL REGISTER notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to GAO.

### § 83.8 Standards of conduct.

(a) GAO employees whose official duties involve the maintenance and handling of personnel records shall not disclose information from any personnel record unless disclosure is part of their official duties or required by statute, regulation, or internal procedure.

(b) Any GAO employee who makes an unauthorized disclosure of personnel records or a disclosure of information derived from such records, knowing that such disclosure is unauthorized, or otherwise knowingly violates these regulations, shall be subject to appropriate disciplinary action. GAO employees are prohibited from using personnel information not available to the public, obtained through official duties, for commercial solicitation or sale, or for personal gain. Any employee who knowingly violates this prohibition shall be subject to appropriate disciplinary action.

### § 83.9 Social Security number.

(a) GAO may not require individuals to disclose their Social Security Number (SSN) unless disclosure would be required—

(1) Under Federal statute; or

(2) 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 SSN as a necessary means of verifying the identity of an individual.

(b) Individuals asked to voluntarily provide their SSN shall suffer no penalty or denial of benefits for refusing to provide it.

(c) When GAO requests an individual to disclose his or her SSN, it shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

### § 83.10 First Amendment rights.

Personnel records or entries thereon describing how individuals exercise rights guaranteed by the First Amendment to the United States Constitution 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