

General Accounting Office

§ 83.8

record, and to instruct each person with respect to such rules and requirements of this part, including any other rules and procedures adopted pursuant to this part;

(i)(1) GAO shall establish and maintain appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of personnel records. At 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;

(2) Except for access by the data subject, only employees whose official duties require and authorize 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 intact on a timely basis and properly controlled during such period of removal.

(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 on-line 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.