and Privacy as soon as it is identified as an appeal under the Privacy Act. An appeal that is improperly addressed shall be deemed not to have been received by the Department until the Office of Information and Privacy receives the appeal, or until the appeal would have been so received with the exercise of reasonable diligence by Department personnel.

(b) *Action on Appeals by the Office of Information and Privacy.* Unless the Attorney General otherwise directs, the Director, Office of Information and Privacy, under the supervision of the Assistant Attorney General, Office of Legal Policy, shall act on behalf of the Attorney General on all appeals under this section, except that: (1) In the case of a denial of a request for access by the Assistant Attorney General, Office of Legal Policy, the Attorney General or his designee shall act on the appeal, and (2) a denial of a request for access by the Attorney General shall constitute the final action of the Department on that request.

(c) *Form of Action on Appeal.* The disposition of an appeal shall be in writing. A decision affirming in whole or in part the denial of a request for access shall include a brief statement of the reason or reasons for the affirmance, including each Privacy Act exemption relied upon and its relation to each record withheld, and a statement that judicial review of the denial is available in the United States District Court for the judicial district in which the requester resides or has his principal place of business, the judicial district in which the requested records are located, or the District of Columbia. If the denial of a request for access is reversed on appeal, the requester shall be so notified and the request shall be processed promptly in accordance with the decision on appeal.

§ 16.49 Preservation of records.

Each component shall preserve all correspondence relating to the requests it receives under this subpart, and all records processed pursuant to such requests, until such time as the destruction of such correspondence and records is authorized pursuant to Title 44 of the United States Code. Under no circumstances shall records be destroyed while they are the subject of a pending request for access, appeal, or lawsuit under the Act.

§ 16.50 Requests for correction of records.

(a) *How Made.* Unless a record is exempted from correction and amendment, an individual may submit a request for correction of a record pertaining to him. A request for correction must be made in writing and must be addressed to the component that maintains the record. (Appendix I to this part lists the components of the Department and their addresses.) The request must identify the particular record in question, state the correction sought, and set forth the justification for the correction. Both the envelope and the request for correction itself must be clearly marked: "Privacy Act Correction Request." If a requester believes that the same record appears in more than one system of records, he should address his request for correction to each component that controls a system of records which contains the record.

(b) *Initial Determination.* Within 10 working days of receiving a request for correction, a component shall notify the requester whether his request will be granted or denied, in whole or in part. If the component grants the request for correction in whole or in part, it shall advise the requester of his right to obtain a copy of the corrected record, in releasable form, upon request. If the component denies the request for correction in whole or in part, it shall notify the requester in writing of the denial. The notice of denial shall state the reason or reasons for the denial and advise the requester of his right to appeal.

(c) *Appeals.* When a request for correction is denied in whole or in part, the requester may appeal the denial to the Attorney General within 30 days of his receipt of the notice denying his request. An appeal to the Attorney General shall be made in writing, shall set forth the specific item of information sought to be corrected, and shall include any documentation said to justify the correction. An appeal shall be addressed to the Office of Information and Privacy, United States Department of Justice, 10th Street and Constitution Avenue, NW., Washington, D.C. 20530, unless the appeal is from a denial by the Assistant Attorney General, Office of Legal Policy, in which case the appeal shall be addressed to the Attorney General, at the same address. Both the envelope and the letter of appeal itself must be clearly marked: "Privacy Act Correction Appeal."

(d) *Determination on Appeal.* The Director, Office of Information and Privacy, under the supervision of the Assistant Attorney General, Office of Legal Policy, or the Attorney General in appropriate cases, shall decide all appeals from denials of requests to correct records. All such appeals shall be decided within 30 working days of receipt of the appeal, unless there is good cause to extend this period. If the denial of a request is affirmed on appeal, the requester shall be so notified in writing and advised of: (1) The reason or reasons the denial has been affirmed, (2) the requester's right to file a Statement of Disagreement, as provided in paragraph (e) of this section, and (3) the requester's right to obtain judicial review of the denial in the United States District Court for the judicial district in which the requester resides or has his principal place of business, the judicial district in which the record is located, or the District of Columbia. If the denial is reversed on appeal, the requester shall be so notified and the request for correction shall be remanded to the component that denied the request for processing in accordance with the decision on appeal.

(e) *Statements of Disagreement.* A requester whose appeal under this section is denied shall have the right to file a Statement of Disagreement with the Office of Information and Privacy, 10th Street and Constitution Avenue, NW., Washington, D.C. 20530, within 30 days of receiving notice of denial of his appeal. Statements of Disagreement may not exceed one typed page per fact disputed. Statements exceeding this limit shall be returned to the requester for condensation. Upon receipt of a Statement of Disagreement under this section, the Director, Office of Information and Privacy, shall have the statement included in the system of records in which the disputed record is maintained and shall have the disputed record marked so as to indicate (1) that a Statement of Disagreement has been filed, and (2) where in the system of records the Statement may be found.

(f) *Notices of Correction or Disagreement.* Within 30 working days of the correction of a record, the component that maintains the record shall advise all components or agencies to which it previously disclosed the record that the record has been corrected. Whenever an individual has filed a Statement of Disagreement, a component shall append a copy of the Statement to the disputed record whenever the record is disclosed. The component may also append to the disupted record any written statement it has made giving the component's reasons for denying the request to correct the record.

§ 16.51 Records not subject to correction.

The following records are not subject to correction or amendment as provided in § 16.50 of this subpart:

(a) Transcripts of testimony given under oath or written statements made under oath;

(b) Transcripts of grand jury proceedings, judicial proceedings, or quasi-judicial proceedings which constitute the official record of such proceedings;

(c) Presentence reports which are the property of the courts, but are maintained by a component in a system of records; and

(d) Records duly exempted from correction pursuant to 5 U.S.C. 552a(j) or 552a(k) by notice published in the Federal Register.

§ 16.52 Request for accounting of record disclosures.

(a) An individual may request a component that maintains a record pertaining to him to provide him with an accounting of those other agencies to which the component has disclosed the record, and the date, nature, and purpose of each disclosure. A request for an accounting must be made in writing and must identify the particular record for which the accounting is requested. The request also must be addressed to the component that maintains the particular record, and both the envelope and the request itself must clearly be marked: "Privacy Act Accounting Request." (Appendix I to this part lists the components of the Department and their addresses.)

(b) Components shall not be required to provide an accounting to an individual to the extent that the accounting relates to: (1) Records for which no accounting must be kept pursuant to 5 U.S.C. 552a(c)(1), (2) disclosures of records to law enforcement agencies for lawful law enforcement activities, pursuant to written requests from such law enforcement agencies specifying records sought and the law enforcement activities for which the records are sought, under 5 U.S.C. 552a(c)(3) and (b)(7), or (3) records for which an accounting need not be disclosed pursuant to 5 U.S.C. 552a (j) or (k).

(c) A denial of a request for an accounting may be appealed to the Attorney General in the same manner as a denial of a request for access, with both the envelope and the letter of appeal itself clearly marked: "Privacy Act Accounting Appeal."

§16.53 Notice of subpoenas and emergency disclosures.

(a) *Subpoenas.* When records pertaining to an individual are subpoenaed by a grand jury, court, or quasi-judicial authority, the official served with the subpoena shall be responsible for ensuring that written notice of its service is forwarded to the individual. Notice shall be provided within 10 working days of the service of the subpoena or, in the case of a grand jury subpoena, within 10 working days of its becoming a matter of public record. Notice shall be mailed to the last known address of the individual and shall contain the following information: The date the subpoena is returnable, the court or quasi-judicial authority to which it is returnable, the name and number of the case or proceeding, and the nature of the records sought. Notice of the service of a subpoena is not required if the system of records has been exempted from the notice requirement of 5 U.S.C. 522a(e)(8), pursuant to 5 U.S.C. 552a(j), by a Notice of Exemption published in the Federal Register.

(b) *Emergency Disclosures.* If the record of an individual has been disclosed to any person under compelling circumstances affecting the health or safety of any person, as described in 5 U.S.C. 552a(b)(8), the individual to whom the record pertains shall be notified of the disclosure at his last known address within 10 working days. The notice of such disclosure shall be in writing and shall state the nature of the information disclosed, the person or agency to whom it was disclosed, the date of disclosure, and the compelling circumstances justifying the disclosure. The officer who made or authorized the disclosure shall be responsible for providing such notification.

§ 16.54 Security of systems of records.

(a) The Assistant Attorney General for Administration, Justice Management Division, shall be responsible for issuing regulations governing the security of systems of records. To the extent that such regulations govern the security of automated systems of records, the regulations shall be consistent with the guidelines developed by the National Bureau of Standards.

(b) Each component shall establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent the unauthorized disclosure of records, and to prevent the physical damage or destruction of records. The stringency of such controls shall reflect the sensitivity of the records the controls protect. At a minimum, however, each component's administrative and physical controls shall ensure that: (1) Records are protected from public view, (2) the area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to the records, and (3) records are inaccessible to unauthorized persons outside of business hours.

(c) Each component shall establish rules restricting access to records to only those individuals within the Department who must have access to such records in order to perform their duties. Each component also shall adopt procedures to prevent the accidental disclosure of records or the accidental granting of access to records.

§16.55 Contracting record systems.

(a) No component of the Department shall contract for the operation of a record system by or on behalf of the Department without the express approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for Administration.

(b) Any contract which is approved shall contain the standard contract requirements promulgated by the General Services Administration to ensure compliance with the requirements imposed by the Privacy Act. The contracting component shall have responsibility for ensuring that the contractor complies with the contract requirements relating to privacy.

§ 16.56 Use and collection of social security numbers.

(a) Each system manager of a system of records which utilizes Social Security numbers as a method of identification without statutory authorization, or authorization by regulation adopted prior to January 1, 1975, shall take steps to revise the system to avoid future collection and use of the Social Security numbers.

(b) The head of each component shall take such measures as are necessary to ensure that employees authorized to collect information from individuals are advised that individuals may not be required to furnish Social Security numbers without statutory or regulatory authorization and that individuals who are requested to provide Social Security numbers voluntarily must be advised that furnishing the number is not required and that no penalty or denial of benefits will flow from the refusal to provide it.

§ 16.57 Employee standards of conduct.

(a) Each component shall inform its employees of the provisions of the Privacy Act, including the Act's civil liability and criminal penalty provisions. Each component also shall notify its employees that they have a duty to: (1) Protect the security of records, (2) ensure the accuracy, relevance, timeliness, and completeness of records, (3) avoid the unauthorized disclosure, either verbal or written, of records, and