Subject: SAFEGUARDING RECORDS CONTAINED IN SYSTEMS OF RECORDS

45-13-00 PURPOSE

A. The Privacy Act of 1974 requires that each Federal agency establish administrative, technical, and physical safeguards to insure the security and confidentiality of records contained in systems of records and to protect the security and integrity of such records against anticipated threats or hazards. This chapter sets forth minimum safeguarding standards for all such records except records maintained in Automated Information Systems (AIS), i.e., records processed by computer.

B. AIS security requirements are described in the Automated Information Systems Security Program Handbook (issued as Part 6 of the HHS Information Resources Management Manual).

45-13-10 SCOPE

The provisions of this chapter apply to all components of the Department, including their contractors, carriers, and intermediaries, that maintain one or more non-automated systems of records, as defined in HHS Exhibit 45-10-A, which are subject to the Privacy Act.

45-13-20 RESPONSIBILITIES

A. Each OPDIV, STAFFDIV, and Regional Office is responsible for the application of the minimum standards set forth in this chapter to its non-automated systems of records and for the development and application of any additional standards which are essential to the safeguarding of the records in such systems. These responsibilities include ensuring that subordinate officials and employees carry out the provisions of this chapter.'

B. Each designated system manager has the primary responsibility for the implementation of these standards for the system(s) of records of which he is manager.

C. Each employee who controls physical access to records or disclosure of information contained in the records is responsible for the specific application of these standards to the records under his control.

D. Each OPDIV or STAFFDIV Privacy Act Officer or Coordinator is responsible for providing overall policy guidance and for ensuring that the published notices of systems of records are periodically updated to properly reflect the implementation of appropriate safeguards, including records disposal schedules and methods.

45-13-30 DEFINITIONS

The definitions applicable to this chapter are contained in Chapter 45-10 (HHS Exhibit 45-10-A: KEY DEFINITIONS APPLICABLE TO THE PRIVACY ACT).

45-13-40 WAIVER PROCEDURE

A. OPDIV and STAFFDIV Heads and Regional Directors may request waivers of specific provisions of these standards. A memorandum requesting a waiver should be addressed to the Assistant Secretary for Public Affairs who is charged with the implementation of the Privacy Act in this Department. The memorandum should describe the nature of the requested waiver, setting forth the rationale supporting the request. This procedure should not be interpreted as providing for a waiver of any provisions of the Privacy Act.

B. The Assistant Secretary for Public Affairs will acknowledge receipt of all requests for such waivers. If the requester does not receive a response within fifteen work days from date of receipt, the waiver should be considered approved.

45-13-50 MINIMUM SAFEGUARDING STANDARDS

A. Risk Analysis

1. An analysis of risks to the records in a system of records should be made not less than once every three years to determine what safeguards are essential to maintain the confidentiality and integrity of the records. Such analysis should be updated whenever: there is a significant change in the sensitivity of the

records: new major uses are made of the records; the records are moved from one storage location to another: new equipment is used to process or store the records; or other circumstances indicate possible increased risk to the records. Some factors to be considered in making a risk analysis are:

a. Sensitivity of the records.

b. Nature of facilities, equipment, and total environment in which the records are maintained.

c. Grade level, experience, and training of personnel who are permitted access to the records.

d. Uses which are made of the records, especially decisions on rights, benefits, and privileges.

e. Uses which others could make of the records if they were inadvertently or intentionally disclosed.

f. Harm that disclosure might cause the record subject.

g. Cost of implementing additional safeguards.

2. Any decisions on safeguards should be based on a judgement that considers such factors. The manager of each system of records should maintain a copy of the last risk analysis on which such decisions are based.

B. Access Restrictions

1. Only those employees who have an immediate need for the records in the performance of their official duties are to have access to such records. As a minimum, access to records must be controlled by an arrangement of the following or equivalent standards:

a. Physically locating the records in areas which are not accessible to unauthorized persons.

b. Stationing security personnel or authorized persons at key access locations.

c. Requiring presentation of an authorized form of identification.

2. Before an employee who will control access to records can work with the records, the supervisor or local official in charge must ensure that the employee is familiar with the safeguards applicable to the records, the access standards in effect, and the Employee Standards of Conduct contained in Appendix A to the Department Privacy Act Regulation (45 CFR 5b).

3. Before any other employee can have access to records, the employee must be fully informed about the safeguards in effect while he has possession of the records. The provisions of Appendix A also apply here.

4. The local official who controls access to records contained in a system of records shall:

   a. Maintain a written procedure for restricting access to the records and a list of employees who control access to the records.

   b. Ensure that each employee who controls access to these records is familiar with this written procedure.

   c. Periodically discuss the procedure with these employees to reinforce their understanding and enforcement of access control.

C. Storage Requirements

1. Very sensitive records, such as those relating to a criminal investigation, are to be kept in lockable metal filing cabinets or in a secured room at all times when not in use during working hours, and at all times during non-working hours. (Each system manager should determine whether the records in a system of records are sensitive to this degree.)

2. Other sensitive records are to be kept in closed containers (e.g., filing cabinets or desk drawers) at all times when not in use during working hours and at all times during non-working hours.

3. Alternative storage facilities may be used provided they furnish an equivalent or greater degree of physical security.

4. Records are not to be left unattended and exposed at any time unless the entire work area is secured from entry by unauthorized persons.

D. Transfer of Records

1. Records are to be transferred in such a way that no accidental dissemination will occur. Small volumes of records are to be transferred by mail in sealed opaque envelopes, including interoffice mail. Sealed containers are to be used to transfer large volumes of records.

2. An employee must not transmit information from records by telephone or fax machine to any employee until the employee's identity and need to know are fully established. Call-back or any other effective procedure for establishing identity may be used. Moreover, highly sensitive information should never be transmitted by these means (unless secure telecommunications technology is available) since there is a considerable risk of unauthorized disclosure.

E. Disposal-of Records

Records are to be disposed of in accordance with the General Records Schedules published by the National Archives and Records Service, or in accordance with the supplementary schedules published by components of the Department.

F. Emergency Operating Plan

A plan for protecting and recovering records in the event of a natural disaster, civil disturbance, or other emergency situation should be maintained for each system of records. The plan should provide for sufficient data back-up capability to ensure continuity of office operations. Employees who work with the records should be made aware of their duties under the plan.

45-13-60 AUDIT

A. Each OPDIV, STAFFDIV, and Regional Office shall audit each of its systems of records at least once every three years for compliance with the standards set forth in this chapter. This audit may be combined as appropriate with the annual review of record keeping practices required by Appendix I to OMB Circular A-130 (Federal Agency Responsibilities for Maintaining Records About Individuals.).

B. Whenever any standard is not being fully met, the system manager must take action during the audit or immediately thereafter to achieve compliance. The system manager shall maintain a copy of the the last audit report as well as a description of corrective actions taken.