CHAPTER 6. APPLICATION OF THE PRIVACY ACT TO OTHER RELATED FUNCTIONS

6-1 Introduction. This chapter sets forth procedures for monitoring the application of the Privacy Act to other related functions. Specifically, monitoring procedures for automated data reporting systems, ADP security, procurement of computer equipment, procurement and contracts, and forms and reports management are addressed.

6-2 Automated Data Reporting Systems. Development of a new or modification of an existing automated reporting system may result in a Privacy Act requirement not heretofore associated with that particular system. (If the records in the system meet the criteria specified in paragraph 1-2, a Privacy Act impact can be expected to result.) Each initiator of an Advanced Requirements Notice (ARN) must indicate whether a Privacy Act impact might result from the new or modified computer system. A brief statement, provided by the initiator, highlighting the impact is to be attached to the ARN.

A. The Systems Engineering Group, (SEG) Office of Information Policies and Systems receives all ARNs for processing. When an ARN is received with Privacy Act impact indicated, SEG will send a copy of the ARN to the Privacy Act Officer for concurrence. If concurrence is obtained, SEG will proceed with normal processing of the ARN request. In those instances where a Privacy Act impact is not indicated on an ARN, but in the judgment of SEG there appears to be an impact (i.e., if the records meet the criteria specified in paragraph 1-2) a copy of the ARN with a statement attached will be forwarded to the Privacy Act Officer for concurrence. Any ARN which involves a computer matching program, as defined in Chapter 5 of this handbook, will be forwarded to the Privacy Act Officer for concurrence.

B. System development efforts initiated in a Field Office that are not using the above AN procedures, which would inform Headquarters, must establish similar procedures. These procedures must, at a minimum provide for evaluation of Privacy Act impact by the Field Office Privacy Act Officer or his designee on each system development effort.

C. System development efforts initiated in Headquarters, including work stations, LANs networks and automated office systems that do not use the ARN procedures, must establish procedures which provide for evaluation of Privacy Act impact by the Privacy Act Officer on each system development effort.

6-3 ADP Security. The protection against unwarranted invasion of personal privacy is a central objective of the Privacy Act. Of particular concern are massive automated files containing personal information bat can easily be retrieved without adequate ADP

security. Security encompasses a management control process that incorporates appropriate administrative, physical and technical safeguards; personnel security; defining and approving security specifications; periodic audits and risk analysis. The Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, is the official document that promulgates policy and responsibilities for the development and implementation of ADP security. "Computer Security Guidelines for Implementing the Privacy Act of 1974," FIPS PUB 41, published by the National Bureau of Standards, U.S. Department of Commerce, is also a good reference. The HUD handbook which addresses security is Handbook 2400.24 REV-1. (Appendix E contains guidelines for establishing safeguards for records subject to the Privacy Act.)

Program Offices (System Owners) are responsible for decisions regarding the security of application systems. IPS will support these decisions and tasks. by interpreting policy, regulations and technical implementation. OMB Circular A-130 states that System Owners are responsible for the security of information systems. It also states the "accountability for information systems should be vested in the officials responsible for operating the programs that the systems support." More specific detailed information regarding System Owners security responsibilities is provided in Handbook 2400.24 REV-1.

A. The Departmental ADP Security Officer is responsible, on behalf of the Assistant Secretary for Administration, for Department-wide implementation of the security portions of OMB Circular No. A-130.

B. The Computer Services Group (CSG), Office of Information Policies and Systems, is responsible for the security of the Department's ADP facilities, and for ensuring that those computer sites which provide services from outside the

Department adhere to any security requirements imposed by HUD.

C. The Systems Engineering Group (SEG), Office of Information Policies and Systems, is responsible for conducting or overseeing design reviews, system tests prior to system implementation and ensuring that security measures are incorporated into systems.

6-4 Procurement of Computer Equipment and Systems The acquisition of new computer equipment and systems which causes a change in the accessibility of the data might affect agency records in such a manner as to have a Privacy Act impact. Such equipment includes hardware, software, remote terminals and non-HUD computers used on a timesharing basis for Departmental functions.

A. The Office of Information Policies and Systems (IPS) has primary technical responsibilities for ensuring that the Privacy Act requirements relating to the procurement have been satisfied.

B. Procurement and rental of computer equipment by a Field Office also must meet Privacy Act requirements. If the procurement is not processed through Headquarters, the Field Office is responsible for ensuring the Privacy Act requirements relating to the procurement have been satisfied.

6-5 Procurement and Contracts. The Department procures a variety of services from the private sector and makes grants to individuals and non-HUD agencies. Many of these procurements may trigger the applicability of Privacy Act requirements. Because of this possibility, each prospective procurement must be examined for the Act's impact. If, in the opinion of the procurement initiator, the Privacy Act may apply to the proposed procurement, this information must be indicated to the Office of Procurement and Contracts.

A. Office of Procurement and Contracts is responsible for reviewing all proposed contract actions for Privacy Act impact, except for the Government National Mortgage Association (GNMA) which is handled by the GNMA Contracting Division. Contracts to which it is anticipated the Privacy Act will apply shall contain a Privacy Act clause, which extends certain provisions of the Act to any contractor operating a system of records to accomplish a Departmental function. The review will consider whether personal information will be collected and whether a system of records will be created.

B. Procurements made by a Field Office also must meet Privacy Act requirements. Each proposed purchase by a Field Office must be reviewed for Privacy Act applicability, and appropriate cases referred to the Field Office Privacy Act Officer or the appropriate designee for a determination as to the Act's impact.

6-6 Forms and Reports Management. There are two separate approving reviews to which data collection efforts are subjected. These two functions often overlap, especially when a reporting requirement is levied by the use of a form. This is covered in the next two paragraphs.

A. In Headquarters, the Forms Management Officer and the Reports Management Officer should not approve any data collection form, reporting requirement or an issuance containing such a form or reporting requirement until the Departmental Privacy Act Officer has first approved it. If this approval has not been obtained on the form, issuance, or reporting requirements, the Forms Management Officer and/or the Reports Management Officer shall forward it to the Departmental Privacy Act Officer.

B. In any Field Office, the Reports Liaison Officer (RLO) and the person designated by the Secretary's Representative and/or the State Coordinator as the Forms Liaison Officer (FLO) should

not approve any internal data collection form, reporting requirement or handbook containing such a form or reporting requirement until the local Privacy Act Officer has first approved it. If the Privacy Act Officer has not seen the form or handbook, a copy should be forward to him first. External reporting requirements are approved by the Departmental Reports Management Officer only.

6-7 The Privacy Conscience of the Department. Appendix G contains guidelines for use by System Managers in developing adequate safeguards to ensure that individual privacy is protected. Any questions concerning the handling of information and/or disclosures should be resolved directly with your local Privacy Act Officer. He will, in addition to the specific duties detailed throughout this Handbook, also be responsible for the following activities:

A. The Departmental Privacy Act Officer will discourage the collection of personal data and the use of data which can be identified with an individual.

1. For new forms:
   a. The Departmental Privacy Act Officer will inspect each form and, working with program officials, establish the need to collect personal data on an individual and how the data will be used before clearing the form for use.

   b. The Departmental Privacy Act Officer will inspect each form and, working with program officials, establish the need to collect the individual's name and/or social security number, and how this identifying information will be used before clearing the form for use.

2. For existing forms and/or systems of records:
   a. The Departmental Privacy Act Officer will inspect each form and/or system of records at the time of its review and obtain suitable justification for the continued need to collect personal data on an individual before clearing the form for continued use.

   b. The Departmental Privacy Act Officer will inspect each form and/or system of records at the time of its review and, working with program officials, establish the continued need to collect the individual's name and/or social security number before clearing the form and/or system of records for continued use. In particular, he will attempt to discontinue the use of the social security number as an identifier unless absolutely necessary, e.g., as used by FHA and GNMA to assist in tracking loans to assure proper risk management.

3. Each Field Office Privacy Act Officer will perform the same review functions on new and existing forms and/or systems of records initiated in his particular Region and/or Field Office. Any questions or need for advice and guidance would be directed to the Departmental Privacy Act Officer.

4. The Departmental Privacy Act Officer, with the assistance of the local office Privacy Act Officers, will attempt to reduce the maintenance of informal, unofficial files

containing personal data on individuals.

5. Appendix G contains guidelines for use by Systems Managers in establishing appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records, and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained by the Department. Additional guidance for Federal computer systems that contain sensitive information is contained in Handbook 2400.24 REV-1, Appendix G.