

Appendix E

RESPONSIBILITIES OF PRIVACY ACT SYSTEMS MANAGERS

E-1 Purpose. This Privacy Act Handbook (Handbook 1325.1) contains detailed information regarding the Privacy Act (the Act) and its implementation in HUD. The list below highlights the most significant responsibilities of the manager of a group of records subject to the Act.

E-2 Responsibilities of the System Manager. The Privacy Act requires that a System Manager be designated by the appropriate Office having responsibility for the system of records. It is the responsibility of the managers of those records to:

A. Initiate action:

1. to provide advance notice to Congress and OMB of intent to establish or alter a Privacy Act system; and,
2. to publish notice in the Federal Register of intent to establish or alter a Privacy Act system.

Prepare draft new/revised systems reports/notices and related documents to ensure that systems of records are not operated without first preparing the required notices and reports. The notices should be submitted to the Privacy Act Officer for review and approval prior to obtaining appropriate Departmental clearance.

- B. Ensure that the published Privacy Act system notice covering the system is current and accurate, with particular emphasis on ensuring that routine use statements are correct and accurate.
- C. Restrict release of records/use of personal information. Do not disclose any record unless disclosure of the record would be:
 1. To those officers and employees of the Department who require the information to perform assigned duties.
 2. Required by the Freedom of Information Act.

E-1

10/95

1325.01 REV-1

3. For a routine use listed in the published Privacy Act system notice. See Appendix 2, Privacy Act, Subsection (b), Conditions of Disclosure, for additional situations in which disclosure is permitted, and for additional information concerning disclosure.

- D. Keep a record ("accounting") of disclosures of information outside the Department (except disclosures made under the

Freedom of Information Act).

1. Retain the record ("accounting") for five years or the life of Privacy Act record, whichever is longer.
 2. Give the record ("accounting") to the subject of the record, upon request.
- E. Establish appropriate safeguards (1) to ensure the security and confidentiality of records, and (2) to protect against any anticipated threats or hazards to their security or integrity (Appendix H contains guidelines for establishing safeguards for records subject to the Privacy Act.)
- F. Maintain only information on an individual that is relevant and necessary to accompany a purpose of the agency required, as required by statute or Executive Order of the President.
- G. Maintain records with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness to an individual in any determination about him.
- H. Keep no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained. The First Amendment protects an individual's right of free assembly, freedom of religion, speech and press, and to petition the Government.
- I. Make reasonable efforts to assure that records are accurate, complete, timely, and relevant before releasing information from a record.
- J. If a record is disclosed containing information about which an individual has filed a statement of disagreement, the system

10/95

E-2

1325.01 REV-1

manager should note the portions of the record under dispute, supply a copy of the statement of disagreement, and, if appropriate, a copy of the Department's reason(s) for not making the requested changes, to the agencies and individuals found in the accounting record.

- K. Inform any recipient of information from a Privacy Act record of any correction or notation of dispute made to the record after the information was released to the recipient.
- L. Attempt to notify the subject of a record if information is released under compulsory legal process.
- M. Collect information directly from the subject to the greatest extent practicable.
- N. Give each individual asked to supply information a Privacy Act Statement. The statement should contain the following

information:

1. The authority authorizing the collection of the information.
 2. Whether the disclosure of the information is mandatory or voluntary.
 3. The principal purpose(s) for which the information is to be used.
 4. The routine uses which may be made of the information.
 5. The effects on the individual, if any, of not providing all or any part of the requested information.
- O. Ensure that all employees who are involved in maintaining the system are aware of their responsibilities for safeguarding the records and maintaining them in accordance with Privacy Act requirements. All HUD Offices have been provided with access to Computer Based Training (CBT) allowing ADP security training to be available on the Local Area Network (LAN). Refer to Handbook 2400.24 REV-1 for additional guidance relating to ADP security training.
- P. Apply Privacy Act requirements to any contractor associated with a system.

E-3

10/95

1325.01 REV-1

- Q. Be sensitive to unique requirements concerning Social Security Number i.e., when individuals are requested to disclose their social security numbers, they must be informed whether that disclosure is mandatory or voluntary, by what statutory or other authority such as number is solicited, and what uses will be made of it.
- R. Use the Systems Development Methodology (SDM) as a reference in the planning, preparation, execution, and administration of HUD's various system development activities and business areas. A copy of the document is available from the Office of Information Policies and Systems (IPS), Systems Engineering Group (SEG), Development Technology Division (DTD) Mainframe Technology Branch.
- S. Be aware of the Criminal Penalties provided in the Act.
1. Any officer or employee who, knowing disclosure of material is prohibited, "--willfully disclosures the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000."
 2. Any officer or employee of any agency who will fully maintains a system of records without meeting the notice requirements shall be guilty of a misdemeanor and fined

not more than \$5,000.

3. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.