HUD Privacy Act Handbook

Directive Number: 1325.1

U.S. Department of Housing and Urban Development
Office of Administration
1325.01 REV-1

TABLE OF CONTENTS

LIST OF EXHIBITS

CHAPTER 1. INTRODUCTION TO THE HANDBOOK

1-1 PURPOSE. This Handbook has two main goals.

A. To provide every employee of the Department with information on their rights and responsibilities under the Privacy Act.

B. To establish policies, procedures, requirements and guidelines for the implementation of the Department's Privacy Act responsibilities.

1-2 RECORDS SUBJECT TO THE PRIVACY ACT (PRIVACY ACT RECORDS). A group of records is subject to the Privacy Act if it satisfies all three of the following criteria:

A. Contains an item, collection, or grouping of information about an individual.

B. Contains name, or identifying number, symbol, or other identifying particular assigned to the individual such as a finger or voice print.

C. Consists of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

1-3 HUD EMPLOYEES AND THE PRIVACY ACT. The Privacy Act imposes requirements on staff members performing in different roles. Each of the roles carries with it special activities with regard to safeguarding the rights of others and carrying out the responsibilities of the Department. The roles are highlighted below:

A. Every employee must safeguard the privacy of every other person, both employee and citizen-client of the Department. This can be accomplished in three ways:

1. Do not let anyone have access to records under your control which contain personal information unless it is: in the performance of official duties (including "routine use" transfers of data); required under the Freedom of Information Act; by direction of a Privacy Act Officer; by direction of the Privacy Appeals Officer (following an appeal of a denial);

or under one of the other conditions of disclosure listed in paragraph 3-5 of this handbook.

2. Purge your files of personal data on individuals as soon as the information is no longer useful, as permitted by law.

3. Minimize the collection of data containing personal information on individuals.

B. Employees responsible for the Office of Human Resources controlled personnel data have three responsibilities in addition to safeguarding individual privacy: to allow an employee access to his or her own personnel records, but under strict supervision to avoid or prevent the possible altering of the official file; to ensure that an employee's right to have a single copy of any or every item in his or her personnel folder is granted; and to ensure that personnel data routed through the mailroom are enclosed in a sealed envelope.

C. Employees responsible for transferring data are likewise responsible for accounting for the disclosure of records containing identifiable personal data on individuals. Such accounting must be made except under the following conditions: transfer to another individual within HUD who uses this information in the performance of his or her official duties;

and transfer of information under the Freedom of Information Act (FOIA) The term "transfer" includes disclosure and divulgence of records and information. from records to any other agency or individual. Detailed information pertaining to disclosure accounting requirements is contained in paragraph 3-6 of this handbook.

D. The Assistant Secretary for Administration is responsible for carrying out the requirements of the Privacy Act, and for establishing such policies and procedures as are necessary for full compliance with the Act.

E. The Departmental Privacy Act Officer within the Office of Information Policies and Systems is responsible for developing, implementing, and interpreting the Department's policies and programs prescribed by the Act and the Office of Management and Budget (OMB) Also, he or she is designated the Privacy Act Officer for Headquarters. The Director, Office of Human Resources, Office of Administration, is delegated authority to act on Privacy Act inquiries and requests for access, copying and correction of records in the Official Personnel Files(OPFs) for employees serviced by Headquarters.

F. Privacy Act Officers are authorized to act on all Privacy Act requests for information, including inquiry, access, change and denial, and are responsible for ensuring that individual rights are protected. The head of each HUD Field Office is designated the Privacy Act Officer. This authority may be redelegated to a staff member.

G. Privacy Act Coordinators are officially-designated Privacy Act representatives within each Headquarters Primary Organization and within each Office of the Assistant Secretary responsible for maintaining liaison with the Departmental Privacy Act Officer, and for representing their organization head in Privacy Act activities necessary to ensure compliance (1) with the Act and (2) with implementing OMB and Departmental requirements. They are also responsible for providing information to be used in responding to OMB reporting requirements and for serving as a contact point in their organization in responding to Privacy Act requests for access to records.

H. The Privacy Appeals Officer is responsible for determining the legal correctness of any denial determination that is appealed. The General Counsel is designated as the Privacy Appeals Officer. The Privacy Appeals Officer for the Office of Inspector General is the Inspector General.

I. Systems Managers are responsible for the policies and practices governing the systems of records they manage and for ensuring that the systems they manage are operated in

compliance with Privacy Act and Departmental requirements. (See Appendix E for additional detail regarding System Manager responsibility for complying with the Privacy Act.)

J. Mailroom employees are responsible for ensuring that all Privacy Act mail, so marked, is sent directly to the appropriate Privacy Act Officer. Privacy Act requests should be handled in the following manner:

1. If an envelope or a letter contains the words "Privacy," "Privacy Act," "Privacy Officer" or combinations of these, it is to be forwarded directly to the Privacy Act Officer in the local Field Office which received the letter. If such is received in Headquarters, it should be sent to the Departmental Privacy Act Officer, Office of Information Policies and Systems.

2. All mail marked "Privacy Appeals Officer" or with similar notations containing the words "Privacy" and "Appeals" should be sent directly to the Privacy Appeals Officer, Office of General Counsel, Washington, D. C. In the Field, this mail is forwarded to the designated Privacy Act Officer for forwarding to the Privacy Appeals Officer.

1-4 CITATIONS AND REFERENCES.

THE PRIVACY ACT OF 1974
(As Amended)

Public Law 93-579

Title 5, United States Code, Section 552a

(usually cited as P.L. 93-579 or 5 USC 552a)

Computer Matching and Privacy Protection Act
Public Law 100-503

IMPLEMENTATION OF THE PRIVACY ACT OF 1974
Rules and Regulations

Title 24, Subtitle A, Code of Federal Regulations, Part 16

(usually cited as: 24 CFR Part 16)

The Privacy Act of 1974 (as amended), 5 USC 552a, is contained in

Appendix C. A guide to the provisions of the Act and the Rules and Regulations, in layman's language and complete with citations and cross-references to the law and the regulations, is contained in Appendix H.

1-5 DEFINITIONS. Both the Privacy Act and the related Departmental regulations use terms which have specific meanings with regard to the procedures for protecting individual privacy. These terms, also used in this Handbook, are defined below to assist you in understanding your rights and responsibilities, and those of the Department, with regard to individual privacy.

A. "Accounting" means the cataloging of disclosures made to any person or agency, public or private. No accounting is required if the disclosure is made to: (1) the subject of the record, (2) HUD employees who have a need to have access to the record in the performance of their official duties, and (3) members of the public as required. by the Freedom of Information Act.

B. "Access" means the process of permitting individuals to see or obtain copies of records about themselves from a Privacy Act system of records. Under the Department's Federal Conduct Rule at 24 CFR Part 9, HUD must make records available to employees in an accessible format. This may include braille, tape, large print, readers, personal computer with voice, etc.

C. "Agency" means any Federal Department, Administration or Office as defined under "Agency" in section 552(e) of Title 5 of the United States Code, Freedom of Information Act. This means this Department, not a component.

D. "Appeal" means the request by an individual to have the Department review and reverse the Privacy Act Officer's decision to deny the individual's initial request for access to, or correction or amendment of, a record of information pertaining to him. The adjudication of an appeal is made by the Privacy Appeals Officer.

E. "Denial of access or correction" means refusal by a Privacy Act Officer to permit the subject of a record to see all or part of this record. Denial of access only can be exercised for records for which an exemption has been published in the Federal Register as part of the description of that system of records. Denial of correction, addition, or deletion of a record is determined by a Privacy Act Officer after fully evaluating all evidence furnished by the individual requesting the record change.

F. "Department" means the U.S. Department of Housing and Urban Development.

G. "Disclosure" means releasing any record or information on an individual by any means of communication to any person or to another agency, public or private.

H. "Him" or "His" means him (her) and his (hers), respectively.

I. "Individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.

J. "Inquiry" means a request by an individual or his legal guardian to have the Department determine whether it has any record(s) of information pertaining to him in one or more of the systems of records covered by the Act.

K. "Maintain" means collect, maintain, use, or disseminate.

L. "Privacy Act" or "Act" means the Privacy Act of 1974, Public Law 93-579 (5 USC 552a).

M. "Privacy Act notice means a statement, imprinted on or attached to a request for personal information, stating; the authority of the Agency to collect the data; the purpose or how the information is to be used; the routine use of or other agencies and individuals that may have access to the data; whether it is mandatory or voluntary on the part of the individual to supply the information; and the penalty, if any, that may be assessed against the individual for not supplying all or part of the information. The information in this Notice permits an individual to make an informed decision as to whether or not to comply with the request for personal information.

N. "Privacy Act Request" means a request by an individual about the existence of, access to, or amendment of a record about himself or herself that is in a Privacy Act system of records. The request does not have to specifically cite or otherwise show dependence on the Act to be considered a Privacy Act request.

O. Record" means any item, collection, or grouping of information about an individual which also includes his name, or any identifying number, symbol, or other particular, such as a finger or voice print, or a photograph. Throughout this Handbook,"Record" refers to each record in a system of records covered by the Act.

P. "Request for access" means a request by an individual or his legal guardian to inspect and/or copy and/or obtain a copy of a record of information pertaining to the subject individual.

Q. "Request for correction or amendment" means the request by an individual or his legal guardian to have the Department change

(either by correction, addition or deletion) a particular record of information pertaining to the subject individual.

R. "Routine use" means the use of a record for a purpose which is compatible with the purpose for which it was collected. Further, it means the record may be disclosed for this purpose without the consent of the subject of the record, to any agency outside the Department which has been identified as having a need for this information and these agencies and individuals have been identified in the Federal Register description of the system of records.

S. "Statistical record" means a record maintained for statistical research or reporting purposes only, and is not to be used in whole or in part in making any determination about an identifiable individual, except as allowed for in Title 13, Section 8, of the United States Code (which refers to the activities of the U.S. Bureau of the Census).

T. "System Manager" means an official who is responsible for the management, operation, and release of information from a system of records subject to the Privacy Act.

U. "System of records" means a group of records under the control of HUD from which information is retrieved by the name of the individual, or by some identifying number, symbol or other identifying characteristic unique to the individual.

CHAPTER 2. INTRODUCTION TO THE PRIVACY ACT

2-1 NECESSITY. Federal agencies collect and disseminate a great deal of personal information about individuals. Records are maintained on employees of the agency, persons doing business with the agency and persons serviced by the agency. In order to safeguard the privacy of individuals from possible infringement, either willful or accidental, by other individuals or public agencies, the Congress of the United States enacted and the President signed Public Law 93-579 on December 31, 1974, entitled the "Privacy Act of 1974." The Act was amended in 1988 to incorporate the requirements for conducting computer matching programs. The Congress stated the following reasons for the necessity of such a law:

A. The privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information.

B. The increasing use of computers and sophisticated -information technology, which is essential to efficient operations and data handling, has greatly increased the possible harm that can occur to an individual's privacy from any collection, maintenance, use or dissemination of personal information.

C. The opportunities for an individual to obtain employment, insurance and credit, and his right to due process under the law and other legal protections are in danger from the possible misuse of certain information systems.

D. The right to privacy is a personal and fundamental right protected by the Constitution of the United States.

E. In order to protect the privacy of an individual who is identified in a Federal information system, Congress must regulate the collection, maintenance, use and dissemination of this information with regard to that system.

2-2 PURPOSE. The objective of the Privacy Act is to provide safeguards for an individual against an invasion of his privacy. In order to accomplish this, the Act requires Federal agencies to follow strict rules of procedure, unless otherwise directed by the law:

A. An individual must be permitted to determine what records pertaining to him are collected, maintained, used or disseminated by Federal agencies.

B. An individual must be allowed to prevent records pertaining to him, that were collected for a specific purpose, to be made available for another purpose without his consent.

C. An individual must be allowed access to information pertaining to him in agency records and to have a copy made of all or any part of that information.

D. An individual must be given the right to seek correction or amendment of" any agency record pertaining to him.

E. The agency may not collect, maintain, use or disseminate any record identifying personal information unless it is for a necessary and lawful purpose.

F. The agency must assure that any information it does collect, maintain, use or disseminate is current and accurate for its intended use, and that adequate safeguards exist to prevent misuse of that information.

G. The agency may exempt records of information from specific requirements of the Act only when an important public policy need for the exemption has been determined by specific statutory authority.

H. The agency will be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under the Privacy Act.

2-3 DEPARTMENTAL POLICY. The U.S. Department of Housing and Urban Development established its policies and procedures for implementing the Act by adopting Part 16, Implementation of the Privacy Act of 1974, as an amendment to Title 24 of the Code of Federal Regulations. Part 16 sets forth the following items of Departmental policy:

A. The Department forbids the collection, maintenance, use or dissemination of secret records. For the purposes of the Privacy Act, secret records are official records containing personal information about individuals; these records are retrieved on the basis of an unique identifier (e.g., name, social security number) corresponding to the individual himself and have not been published in the Federal Register.

B. The Department will ensure the protection of individual privacy by safeguarding against the unwarranted disclosure of records containing information on individuals.

C. The Department will act promptly on any request for information about, for access to or for appeal against a decision concerning records containing information on individuals, which is made by a citizen of the United States or an alien lawfully admitted for residence into the United States, regardless of the age of the individual making the request or the reason for the request.

D. The Department will maintain only information on individuals which is relevant and necessary to the performance of its lawful functions.

E. The Department is responsible for maintaining information on individuals with such accuracy, relevancy, timeliness and completeness as is reasonably necessary to assure fairness to the individual in any determinations that are made.

F. The Department will make every effort to obtain information about an individual directly from the individual.

G. The Department will not maintain any record describing how an individual exercises his or her rights guaranteed by the first Amendment (freedom of religion, speech and press, peaceful assemblage, and petition of grievances), unless expressly authorized by statute or by the individual.

H. The Department will ensure an individual the right to seek the correction or amendment of any record in a system of records pertaining to him or her.

I. The Department will review upon appeal all decisions that deny access to or corrections and amendments of records under the Act.

J. **The Department requires all organizational components to follow the same rules and procedures to assure uniformity and consistency in implementation of the Privacy Act.**

K. **With respect to requests for information, the Department will disclose the maximum amount of requested information within the constraints of legality.**

2-4 YOUR RESPONSIBILITIES. As an employee of the Department you have certain responsibilities to assist the Department in safeguarding your rights and those of others. These responsibilities, for which you' are held accountable by law, are listed below:

A. **Do not disclose any record contained in a system of records by any means of communication to any person, or another agency except under the specific conditions of disclosure stated in the Act and in Departmental regulations.**

B. **Do not maintain unreported files which would come under the Act. Paragraph 4-3 describes reporting requirements.**

C. **Do not maintain records describing how any individual exercises his or her rights guaranteed by the, First Amendment unless expressly authorized by statute or by the individual. The First Amendment protects an individual's rights of free assembly; freedom of religion, speech and press; and to petition the Government.**

D. **Privacy rules that will help you avoid the difficulties associated with Items A., B., and C., above, are the following:**

1. **Safeguard the privacy of all individuals and the confidentiality of all personal information.**

2. **Report the existence of all personal information systems not published in the HUD Privacy Systems Notice to your Privacy Act Officer.**

3. **Account for all transfers of personal records outside the Department. See paragraph 3-6.**

4. **Limit the availability of records containing personal information to Departmental employees who need them to perform their duties.**

5. **Avoid unlawful possession of or unlawful disclosure of individually identifiable information.**

E. **All HUD program office Records Management Liaison Officers (RMLOs) must ensure that retention and disposition schedules**

are in place for records in their specific program areas covered by the Privacy Act systems of records. Existing records disposition schedules can be found in Handbooks 2225.6 REV-1, HUD Records Disposition Schedules; and 2228.2 REV-2, General Records Schedules.

2-5 Criminal Penalties. The Privacy Act provides the following penalties for unauthorized disclosure of records. All three are misdemeanors punishable by fines of $5,000.

A. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by the Privacy Act or by rules or regulations of the Department, and who knowing that disclosure of the specific material is so prohibited, will fully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor.

B. Any officer or employee of HUD who willfully maintains a system of records without meeting the notice requirements in paragraph 4-3 of this handbook shall be guilty of a misdemeanor.

C. 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.

CHAPTER 3. PROCEDURES FOR PROCESSING AND MONITORING REQUESTS FOR RECORDS SUBJECT TO THE PRIVACY ACT

3-1 Introduction. This chapter sets forth procedures for processing requests for access to or amendment of records under the Privacy Act. It also includes procedures for disclosing records, and accounting for such disclosures.

3-2 Personnel involved in Privacy Act activities fall into two categories: those who process" and disclose information and those who make decisions concerning the disclosure of the information. The first category includes mailroom personnel and persons responsible for transmitting information and accounting for the disclosures. Mailroom employee responsibilities are discussed in paragraph 1-3. Procedures for processing requirements relating to making decisions concerning the disclosure of the information is discussed in this chapter. However, any questions concerning the handling of information and/or disclosures should be resolved directly with the Privacy Act Officer.

3-3 Relationship between the Privacy Act and the Freedom of Information Act (FOIA) In some instances individuals requesting access to records pertaining to themselves may not know which Act to cite as

the appropriate statutory authority. The following guidelines are to ensure that the individuals receive the greatest degree of access under both Acts:

A. Any person may use the FOIA to request access to agency records. This includes U.S. citizens, permanent resident aliens, foreign nationals, corporations, unincorporated associations, universities, and state and local governments. The FOIA enables a person to obtain access to agency records. Only those records that are not maintained by the requester's identifier and hence not "records" within "systems of records" are available under FOIA.

B. Only individuals may use the Privacy Act. "Individual" is limited to U.S. citizens and aliens lawfully admitted for permanent residence. The Privacy Act in addition to access, establishes a right to correct, amend, or expunge records about an individual that are not accurate, relevant, timely and complete. Only records that are retrieved by the individual's personal identifier and not exempt from access as described in paragraph 3-11 are releasable.

3-4 Choosing the Appropriate Act. When making a decision regarding which Act to process requests for information the following factors should be considered.

A. If the request is from an individual seeking information pertaining to him, cites only the Privacy Act, and the responsive documents are contained in a systems of records pertaining to the requester, the request should be processed, under the Privacy Act, taking into account any exemptions available under the statute.

B. If the request cites only the FOIA, requests information about a project, a program, an organization, etc., it should be processed under the FOIA, taking into account only those exemptions under the FOIA. See the FOIA handbook 1327.1, REV-1, for more specific details relating to FOIA procedures and processes. Additional guidance on FOIA exemptions which allows the Department to withhold certain information can be obtained from the Freedom of Information Officer in the Office of Executive Secretariat.

C. If the requester cites both the Privacy Act and the FOIA, process it under the Act that provides the greater degree of access.

D. Do not penalize the individual access to his records otherwise releasable, solely because he failed to cite the appropriate statute or instruction.

3-5 Exemptions from the Privacy Act. The Privacy Act permits certain

types of systems of records to be exempt from access and other provisions of the Act. There are ten exemptions which are described at 5 U.S.C. 552a (d) (5), 5 U.S.C. 552a(j) and 5 U.S.C. 552a (k) See Appendix C, The Privacy Act of 1974, as amended, for a detailed description of all of the exemptions. Whether a system of records may be exempted is based on the purpose of the system of records, not the identity of the organizational component maintaining the records. When it is determined that a system of records should be exempted from certain provisions of the Act, a proposed rule must be published in the Federal Register naming the system and stating the specific provisions of the Act from which the system is to be exempted and the reasons. After a 30 day period for public comment, a final rule must be published in the Federal Register. Agencies may not withhold records under an exemption until these requirements have been met. The Privacy Act Officer should be contacted for further guidance on whether or not a system of records should be exempted and for assistance in preparing the appropriate documents required for the Federal Register Notices.

3-6 Conditions of Disclosure. The Privacy Act prohibits the Department from disclosing any record contained in a system of records in any way to anyone without a written request from or prior written consent from the individual concerned in the record, unless disclosure is for one of the following purposes:

A. Performance of duties by the officers and employees of the Department.

B. Required in response to a request under the Freedom of Information Act, Title 5, Section 552 of the United States Code.

C. Routine use, as defined in 1-5, R., where the routine use and the purpose of such use have been published in the Federal Register.

D. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13.

E. To a recipient who has provided HUD with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is disclosed in a form that is not individually identifiable. This exception is limited to records which, even in combination, cannot be used to identify individuals.

F. To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or his

designee to determine whether the record has such value.

G. To another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a criminal or civil law enforcement activity if the activity is authorized by law and if the head of the agency or instrumentality has made a written request to the agency maintaining the record specifying the particular portion desired and the law enforcement activity for which the record is sought. The head of an agency, for purposes of this condition of disclosure, means an official of the requesting law enforcement agency at or above the rank of section chief or equivalent.

H. The health or safety of an individual, and then only if the person making the request, has shown a "compelling circumstance" and notification of the disclosure is sent to the individual's last known address.

I. To either house of Congress, or, to the extent of matters within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee or any such joint committee. This does not authorize the disclosure of a Privacy Act record to an individual member of Congress acting in his own behalf or on the behalf of a constituent.

J. To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office.

K. Required by the order of a court of competent jurisdiction. Keep in mind, however, that a subpoena routinely issued by a court clerk is not acceptable, as it must be signed by a judge.

L. To a consumer reporting agency in accordance with section 3711(f) of title 31. A consumer reporting agency is a person or business which assembles and evaluates information for third parties or makes/markets credit reports. A routine use must be established prior to disclosing information to a consumer reporting agency. Prior to disclosure, the agency head must determine that a valid claim exists and inform the individual: that the debt is overdue; that the agency intends to notify a consumer reporting agency; what information will be released; and that the individual may seek a full explanation of the claim, dispute the claim and appeal the initial agency decision with respect to the claim.

3-7 Accounting for Certain Disclosures. The Privacy Act requires agencies to keep an accounting of disclosures made from its systems of records so that it is simpler to trace data to be corrected, and

to inform individuals about disclosures made and to monitor compliance. Accounting for disclosures means to record in some way what was disclosed and to whom. Thus, any employee who discloses such information must maintain a record of account. It is not necessary to account for disclosures that transfer records to another individual within HUD who uses the information in the performance of his official duties or the FOIA. In the event that a request for access is received from an agency that is not listed under "routine use" or an individual who is not the subject of the requested record, prior consent must be obtained from the subject individual each and every time before that disclosure can be made. See Exhibit 3-1 for a sample letter that may be used to inform the subject individual of the request and Exhibit 3-2 for a sample form that may be used to obtain consent.

A. Content of Accounting Records. The accounting record must include the date, nature, and purpose of the disclosure, and the name and address of the recipient. It must be kept for 5 years after the disclosure is made or the life of the record, whichever is longer. Also, the individual must be given access to the disclosure accountings about him. See Exhibit 3-3 for a sample form that may be used for recording accounting disclosures.

B. Maintaining Disclosure Accounting Records. Disclosure accounting records are official office records and must be kept available for reference and review. They are to be maintained by the Office, Division or Branch that maintains the disclosed information. Specific details of the disclosed records should be recorded.

3-8 Inquiries Concerning Systems of Records. Anyone may inquire into the existence of a record of information pertaining to one's self or to a dependent child or legal ward in a system of records maintained by the Department. Privacy Act Officers should attempt to honor oral requests whenever possible, but in the event of questions on the validity of the request, the Privacy Act Officer should have a request submitted in writing.

A. Inquiries should contain the following information: Name, address and telephone number of the requester; name, address and telephone number of the individual to whom the record pertains, if the individual is a minor or legal ward of the requester; a certified or authenticated copy of documents establishing parentage or guardianship, if such is necessary, whether the individual to whom the record pertains is a citizen or an alien lawfully admitted for residence into the United States; name and location of the system of records as published in the Federal Register; any additional information that might assist the Department in responding to the inquiry; date of the inquiry; the requester's signature. Exhibit 3-4 contains a sample Privacy Act request letter.

1. If an inquiry is misdirected, the Departmental official receiving it should promptly refer it to the appropriate Privacy Act Officer; the time of receipt for processing purposes is the time that the Privacy Act Officer receives the inquiry. The requester should be informed of the transfer. See Exhibit 3-5 for a sample letter informing the requester of the transfer of a Privacy Act Request to the appropriate HUD office.

2. An historical log should be maintained by each Privacy Act Officer for each case handled in his office. Appendix A presents a Privacy Act Case Log for this purpose, which should be started at the beginning of each calendar year and retained for an additional calendar year.

3. If a requester does not know the name of the system of records he is concerned about, the Privacy Act Officer will provide assistance either in person or by mail.

4. If an inquiry fails to contain all necessary information, the Privacy Act Officer will inform the requester that the time of receipt for processing purposes will be the time when the additional necessary information is received. See Exhibit 3-6 for a form letter that may be used to obtain the additional information.

5. Once there is sufficient information to process the request, a record search procedure must be initiated. This involves contacting the HUD staff(s) that maintain(s) the system(s) of records. Exhibit 3-7 contains a Record Search Procedure Log that may be used to retain a history of this activity.

6. The Privacy Act Officer should make every effort to respond to an inquiry within 10 working days of receipt of the inquiry. If a response cannot be made within 10 working days, the Privacy Act Officer will notify the requester of this fact and provide him with an estimate of when the request would be satisfied, as well as the reason for the delay. See Exhibit 3-8 for a sample letter that may be used for this purpose.

7. Paragraphs 3-8 through 3-16 relate to the processing of the various types of Privacy Act requests and the Departmental responsibilities with respect to them. Exhibit 3-9 contains a sample letter by which the requester can be informed of the Departmental action taken with respect to his request and the actions he must take to obtain the information that was requested, if such are necessary.

3-9 Individual Requests for Access to Information Maintained in Systems of Records.

A. Individual Rights. Any individual may request access to records maintained about him by the Department. The Department must, upon request:

1. Inform an individual whether a system of records contains a record or records pertaining to him;

2. Permit an individual to review any record pertaining to him which is contained in a system of records;

3. Permit the individual to be accompanied by a person of his choosing; and

4. Permit the individual to obtain a copy of any such record in a form comprehensible to him at a reasonable cost. This may include braille, tape, large print, readers, personal computer with voice, etc. No additional fee may be requested from an employee with a disability who requests material in an accessible format.

B. Agency Responsibilities. Privacy Officers should attempt to honor oral requests whenever possible, but may ask that the request be submitted in writing. In the event that a request is misdirected to a HUD office, the Privacy Act Officer should transfer the request to the appropriate office and notify the requester of the transfer. See Exhibit 3-5 for a sample letter that may be-used to inform the requester of a transfer to the appropriate HUD Office.

3-10 Verification of Identity. The Privacy Act requires agencies to develop procedures to verify the identity of a person requesting to see or copy his record, but such requirements should not be unduly burdensome. The purpose is to reasonably ensure that a person" is not improperly granted access to the records of another. The following procedures should be followed before granting oral and written requests for access to records.

A. An oral request for access must be accompanied by the following identification:

1. A document bearing the requester's photograph (building pass, license, etc.).

2. A document bearing the requester's signature.

3. In the event of no such document, a signed statement asserting the requester's identity and stipulating that the requester understands the penalty provisions of the

Act. See Exhibit 3-10 for an example of such a statement.

4. If the requester is a parent or legal guardian of the individual to whom the record pertains, the Privacy Act Officer must also obtain proof of identification through a certified or authenticated copy of the court's order in the case of a ward. In no event can a parent or guardian act for a decedent. However, access to Office of Human Resources records maintained by the Department may be granted to a survivor of a deceased employee, or annuitant or someone acting in his behalf.

5. In order to facilitate processing, the Privacy Act Officer should also determine if the request for access is a result of an earlier inquiry.

B. Written request for access should contain the same identifying information as required for an oral inquiry. Proof of identity should be established by a certificate of a notary public or equivalent officer empowered to administer oaths.

C. Whether the request for access is oral or in writing, the following will apply;

1. If the request is misdirected the Department official receiving it will promptly refer it to the appropriate Privacy Act Officer; the time of receipt of the request for processing purposes is the time the Privacy Act Officer receives it.

2. If the request fails to contain all the necessary information and documents, the Privacy Act Officer will inform the requester that the time of receipt for processing purposes will be the time when he provides the additional information. See Exhibit 3-6 for a sample letter that may be used for this purpose.

3. Once, in the opinion of the Privacy Act Officer, there is sufficient information to process the request, a record search procedure must be initiated. This involves contacting HUD staff(s) that maintain(s) the system(s) of records. Exhibit 3-7 contains a Record Search Information Log that may be used to retain a history of this activity.

4. The Privacy Act Officer will respond to a request within 10 working days of receipt of the request. If a response cannot be made within 10 working days, the Privacy Act Officer will notify the requester of the estimated date that a response can be made and the reason for the delay. See Exhibit 3-8 for a sample letter that may be used for

this purpose.

5. The requester shall not be required to state a reason or otherwise justify his request for access to a record.

D. If the record is contained in a personnel file under control of the Office of Human Resources, the request can be made directly to the appropriate Personnel Officer who will act for the Privacy Act Officer in this case.

3-11 Disclosure of Requested Information to Individuals. Under the Privacy Act, an individual has access to records only if those records are within a system of records; i.e., the records are retrieved by the individual's name or other identifier.

A. Upon granting access to a record in response to a request for access the Privacy Act Officer will notify the requester in writing, providing the following information:

1. The time and place where the records will be available for personal inspection, and the period of time that the records will be available for inspection;

2. A copy of the information requested if no fees are involved;

3. An indication of whether the copy will be held pending receipt of fees to cover the cost of copying documents, and the estimate of the fee for copying the record;

4. An indication that the requester may be accompanied by another individual during the period of access and the procedures required to allow that individual access to the record. See paragraph 3-11; B., 4.;

5. And, any additional requirements needed to grant access to a specific record.

B. The Privacy Act Officer will also ensure that:

1. Manual record files are the source for disclosing the information and for copying purposes unless a computer printout of the record is both easily available and readable (clear English).

2. Any information or assistance that is needed to make the record intelligible will be provided at the time of access.

3. Original records will only be available under the immediate supervision of the Privacy Act Officer or his designee and that copies or abstracts may be available to

guarantee the security of the original record.

4. When the requester is accompanied by another person(s), the individual to whom the record pertains will authorize the presence of that other person, in writing, including the name of the individual and the record to which access is sought, sign the authorization and have the accompanying individual sign the authorization in the presence of the Privacy Act Officer (see* Exhibit 3-11 for an example of such an authorizing document).

3-12 Initial Denial of Access to Records. The Privacy Act Officer may not deny an individual access to any record pertaining to the individual except under highly selective conditions.

A. Grounds for denial of access to an individual's record(s) follows:

1. The record is in a system of records which the Department has exempted from access or in a system of records exempted by another agency responsible for filing a notice on the system. The exemption status of a system of records is found in the individually published system of, records notice.

2. The record was compiled in reasonable anticipation of a civil action or proceeding.

3. The individual has unreasonably failed to comply with procedural requirements for requesting access.

B. Notification of denial of a request for access must be in writing and should include the following information:

1. The Privacy Act Officer's name and title or position.

2. The date of the denial.

3. The reason(s) for the denial, including citation to the appropriate section(s) of the Act and the Departmental regulations.

4. The individual's opportunity for an administrative review of the denial through a Departmental appeal procedure, which includes a written request for review within 30 calendar days that contains copies of the original request for access, and a statement of why the denial is believed to be in error.

5. The name and address of the Departmental Privacy Appeals Officer.

6. If the denial is administratively final (that is, no opportunity for an appeal), then state the individuals right to judicial review, including citation of the appropriate section(s) of the Act and the Departmental regulations. This can occur when the request for access is to another agency's record in your possession which has been exempted by them under the provisions for a "General Exemption."

3-13 Appeal of Initial Denial of Access to Records. The Privacy Appeals Officer will review any initial denial of access to records only if a written request for the review is filed within 30 calendar days from the date of the notification of denial of access to the record.

A. The appeal package must contain:

1. A copy of the request for access.

2. A copy of the written denial of the request for access.

3. A statement of the reasons why the initial denial is believed to be in error.

4. The individual's signature.

B. The procedures and processing relating to appeal requirements are contained in Appendix D.

3-14 Request for Correction or Amendment to a Record. Any individual may submit a request to the Department for correction or amendment of a record pertaining to that individual, or to a dependent child or legal ward. Privacy Act Officers should attempt to honor oral requests whenever possible, but they may require that the request be submitted in writing.

A. The request for correction or amendment should include the following information:

1. A specific identification of the record sought to be corrected or amended.

2. The specific wording to be deleted, if any.

3. The specific wording to be added, if any, and the exact place at which it is to be inserted or added.

4. A statement of the basis for the requested correction or amendment, including all available supporting documents or materials which substantiate the statement.

5. Since the request, in all cases, will follow a previous

request for access, the individual's identity will be established by his signature on or accompanying the request.

B. Upon receipt of the request for correction or amendment to a record, the Privacy Act Officer will make a determination within 10 working days, to do one of the following:

1. Make the requested correction or amendment and notify the individual of the action taken;

2. Acknowledge receipt of the request and provide an estimate of time within which action will be taken, explaining to the requester any unusual circumstances (such as, records are in inactive storage, field facilities or other establishments; voluminous data are involved, information on other individuals must be separated or deleted; consultation with other agencies having a substantial interest in the determination are necessary). The Privacy Act Officer may also ask for such further information as may be necessary to process the request; or,

3. Inform the individual in writing that the request is denied.

C. Upon receipt of further information that may have been requested, the Privacy Act Officer will acknowledge within 10 working days and promptly determine to do one of the following:

1. Make the requested correction or amendment and notify the individual of the action taken, providing, when feasible, a copy of the corrected or amended record.

(a) If the uncorrected record has been disclosed to a person or an agency and an accounting was made of the disclosure, the Privacy Officer will notify all such persons and agencies of the correction or amendment.

(b) A recipient agency maintaining the record must acknowledge receipt of the notification, correct or amend the record, and notify any other person or agency to whom it has disclosed the record, providing an accounting was made of the disclosure, of the substance of the correction or amendment.

2. Inform the individual in writing that the request is denied.

3-15 Criteria for Considering a Request for Correction or Amendment.

The Privacy Act Officer will consider the following criteria in making a determination on a request to correct or amend an individual's record:

A. The sufficiency of the evidence submitted by the individual.

B. The factual accuracy of the information.

C. The relevance and necessity of the information in terms of purpose for which it was collected.

D. The timeliness and currency of the information in terms of the purpose for which it was collected.

E. The completeness of the information in terms of the purpose for which it was collected.

F. The possibility that denial of the request could unfairly result in determinations adverse to the individual.

G. The character of the record sought to be corrected or amended.

H. The propriety and feasibility of complying with the specific means of correction or amendment requested by the individual.

3-16 Initial Denial to Correct or Amend a Record. The Privacy Act Officer may not deny an individual the right to correct or amend the contents of a record pertaining to the individual except under highly*selected conditions.

A. Grounds for denial of a request to correct or amend an individual's record(s) follow:

1. The evidence presented has failed to establish the propriety of the correction or amendment when weighed against the applicable criteria set forth in paragraph 3-11. The Privacy Act Officer will not undertake to gather evidence for the individual, but does have the right to verify the evidence submitted.

2. The record sought to be corrected or amended was compiled in a terminated judicial, quasi-judicial, legislative or quasi-legislative proceeding to which the individual was a party or participant.

3. The information in the record sought to be corrected or amended or the record sought to be corrected or amended, is the subject of a pending judicial, quasi-judicial or quasi-legislative proceeding to which the individual is a party or participant.

4. The correction or amendment would violate a duly enacted

statute or promulgated regulation.

5. The individual has unreasonably failed to comply with the procedural requirements for requesting a correction or amendment to a record.

B. Notification of denial of a request to correct or amend a record must be in writing and will include the following information:

1. The Privacy Act Officer's name and title or position.

2. The date of the denial.

3. The reason(s) for the denial, including citation of the appropriate section(s) of the Act and the Departmental Regulations.

4. The procedures for a Departmental appeal.

5. The name and address of the Departmental Privacy Appeals Officer.

3-17 Appeal from Initial Denial to Correct or Amend a Record. The Privacy Appeals Officer will review any initial denial to correct or amend a record only if a written request for review is filed within 30 calendar days from the date of the notification of denial to correct or amend the record. The procedures and processing requirements relating to appeals are contained in Appendix D.

3-18 Reproduction Fees. Generally only one copy of any record or document will be provided. Checks or money orders for fees should be made payable to the "Treasurer of the United States". Fees should only include the direct cost of reproduction.

A. No fees should be charged for the following:

1. Time or effort devoted to searching for or reviewing the record by HUD personnel;

2. Fees not associated with the actual cost of reproduction;

3. Producing a copy when it must be provided to the individual without cost under another regulation, directive, or law;

4. Normal postage;

5. Transportation of records or personnel; or

6. Producing a copy when the individual has requested only to review the record and has not requested a copy to

keep, and the only means of allowing review is to make a copy (e.g., the record is stored in a computer and a copy must be printed to provide individual access or the HUD official does not wish to surrender temporarily the original record for the individual to review).

B. Copying fees will be charged as prescribed below:

1. Each copy of each page, up to 8 1/2 X 14 made by photocopy or similar process - $0.15.

2. Each page of computer printout, without regard to the number of carbon copies concurrently printed - $0.20.

3. Micrographic copy:

a. duplicating - per fiche: $1.00

b. duplicating 16 mm roll $2.00 per roll/cartridge

c. paper print out - from microfilm/microfiche: $0.15 per image/page.

C. Fee Waiver. A copy fee of $1.00 or less shall be waived by the Privacy Act Officer, but the copying fees of several simultaneous requests by the same individual will be aggregated to determine the total fee. The Privacy Act Officer may elect to reduce a fee or to eliminate it completely if he deems it to be in the public interest; such as, when the cost to the Government to process the fee disproportionally exceeds the amount of the fee.

EXHIBIT 3-1 SAMPLE LETTER TO INFORM INDIVIDUAL OF A REQUEST FOR ACCESS TO HIS PERSONAL INFORMATION

(Name)
(Address)
SUBJECT: Letter to Inform Individual of a Request for Access to his personal information

Dear _____,

On (date), the U.S. Department of Housing and Urban Development received a request from (Name and address of requesting official or agency) to disclose a record(s) about you, as described below. Since this record comes under the Privacy Act of 1974, we may not disclose the record to this individual or agency without your knowledge. Your consent is necessary before such disclosure can be made.

Please complete the attached consent form and return it notifying

us of your decision on this matter.

Sincerely,

Privacy Act Officer

DESCRIPTION OF REQUEST: (State type of record/information and reason/use for request)

EXHIBIT 3-2 SAMPLE FORM TO OBTAIN CONSENT TO DISCLOSE PERSONAL INFORMATION

I, _____, hereby () grant / () refuse (check one) permission to the U.S. Department of Housing and Urban Development to disclose my record, as described in the attached, to (name of individual or agency), in response to a request dated _____ from this person or agency for disclosure of such record. No subsequent disclosure of such record to the individual or to any other individual or agency is to be made without my additional explicit consent, except as may be authorized by law.

_____
signature

_____
Date

EXHIBIT 3-3 SAMPLE FORM FOR RECORDING ACCOUNTING DISCLOSURES DISCLOSURE ACCOUNTING FORM RECORD OF DISCLOSURE UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM THIS RECORD COULD SUBJECT THE DISCLOSURE TO CRIMINAL PENALTIES

1. **This is to remain a permanent part of the record described below**
2. **An entry must be made each time the record or any information from the record is viewed by, or furnished to any person or agency except:**
   A. A disclosure to HUD personnel having a need to know in the performance of official duties; or,
   B. When required under the Freedom of Information Act.

Date of Disclosure	Method of Disclosure	Purpose or Authority	Name & Address of Person or or Agency to whom disclosed information, with signature if made in person.

EXHIBIT 3-4 SAMPLE PRIVACY ACT REQUEST LETTER

Privacy Act Officer
Department of Housing and Urban Development
451 7th Street SW
Washington, DC 20410

Dear Sir:

Under the provisions of the Privacy Act of 1974, I am requesting a copy of all records the Department is presently maintaining on me. I was employed by the HUD Regional Office in San Francisco as a contractor during the period of 1979 through 1985. The company that I was working with was the X Company of San Francisco. I am interested in any records relating to my performance as a contractor, the awarding of the contract, the termination of the contract, and the subsequent loss of my job. Information verifying my identity is resented below.

Mr. John Doe
777 Block Avenue
San Francisco, CA 22222
Telephone No.: (415) 555-8888

I am enclosing a notarized copy of some documents of identification. Please send the information to the above address. You may call me if you have further questions.

I look forward to an expeditious response to my inquiry. Thank you for your assistance.

Sincerely,

John Doe

Enclosures

EXHIBIT 3-5 SAMPLE LETTER INFORMING REQUESTER OF TRANSFER OF PRIVACY ACT REQUEST TO APPROPRIATE HUD OFFICE

(Name)
(Address)

Dear _____,

The information that you recently inquired about has been found in a Privacy Act System of records that is maintained at another HUD office. Your request is being transferred to that office for further handling. Your contact at that office is:

(Name)
(Privacy Act Officer)
(Business address)

You may expect to hear from him shortly.

Sincerely,

(Departmental) Privacy Act Officer

EXHIBIT 3-6 SAMPLE LETTER USED TO OBTAIN ADDITIONAL INFORMATION

Case No.:

(Name)
(Address)

Dear _____,

We have received your request under the Privacy Act of 1974, and need additional information before we can comply with your request. Please complete the items below and return to the undersigned Acting Privacy Act Officer.

What was your relationship with HUD at the time the record was created (such as, employee or prospective employee, mortgage insurance applicant, mortgagor, builder or developer, contractor or prospective contractor, etc.):

_____
_____

Approximate date when the record was created:
_____

Address when record was created:
Street No: _____
City, State, ZIP: _____

Additional Information that may assist HUD in complying with your request (such as, date of birth, names of parents, place of work, dates of employment, position, title, etc.) :

_____
_____

Please note that the time of receipt for processing purposes will be the time that this additional information is received in our office. Thank you.

Very sincerely yours,

(Departmental) Privacy Act Officer

EXHIBIT 3-7 SAMPLE RECORD SEARCH INFORMATION LOG

U.S. Department of Housing and Urban Development
RECORD SEARCH INFORMATION
Case No: _____

Date of	Name of	Location of	Type of Action

Action Person Contacted Person Contacted and remarks

EXHIBIT 3-8 SAMPLE LETTER FOR PRIVACY ACT PROCESSING OVER 10 DAYS

Case Number_____

(Name)
(Address)

Dear _____,

Your request under the Privacy Act of 1974 has been received and is being processed. You will receive a response within _____.

Your response is delayed because
_____
_____
_____
_____.

If you need to contact us further on this request, please use the Case Number referred to on the upper right side of this letter.

EXHIBIT 3-9 SAMPLE LETTER TO INFORM REQUESTER OF DEPARTMENTAL ACTION

Case No.:_____

(Name)
(Address)

Dear _____,

We have received and processed your request under the Privacy Act of 1974. (Type the one of the following that applies:)

We do not have a record pertaining to you in the following Privacy Act System of Records: (Name of SOR)

We do not have a record pertaining to you in a Privacy Act System of Records.

Your request for access to a record is granted. A copy of the record is enclosed. Please contact the undersigned Privacy Act Officer to arrange a suitable time to inspect the record.

Your request for access to a record is denied because it is exempt from disclosure. The procedure to exercise your right of appeal of this denial is attached.

Your request to correct or amend a record is granted: A copy of the corrected/amended record is enclosed. Please contact the undersigned Privacy Act Officer to arrange a suitable time to inspect the corrected/amended record.

Your request to correct or amend a record is denied because (state reason). The procedure to exercise your right of appeal of this denial is attached. Enclosed is a copy of the accounting of disclosures of your record, as you requested.

A fee of (state amount) will be charged to make a copy of your record as you requested. Please make a check or money order payable to "Treasurer of the United States" and present it to the undersigned Privacy Act Officer or his designee.

Sincerely,

(Departmental) Privacy Act Officer

EXHIBIT 3-10 SAMPLE STATEMENT OF IDENTITY

City:
County:
Social Security Number:

(Name of individual) who fixed his signature below in my presence, came before me, a (title), in and for the aforesaid County and State, this (date) day of (month, year), and established his identity to my satisfaction. My Commission expires (date).

_____
Signature

EXHIBIT 3-11 SAMPLE REQUESTER'S AUTHORIZATION FOR AN ACCOMPANYING INDIVIDUAL

I (name) grant permission for the following named individual(s) _____ _____ _____ to accompany me while I have access to personal information about me, contained in the following system(s) of records:
_____
_____
_____.

Signed: (requester)

Signed: (accompanying individual(s)

_____

_____

Witnessed: _____ _____

Privacy Act Officer **Date**

CHAPTER 4. ESTABLISHING AND MANAGING PRIVACY ACT SYSTEMS OF RECORDS

4-1 Introduction. This chapter sets forth procedures for establishing and managing systems of records under the Privacy Act. The Privacy Act of 1974 requires agencies to publish in the Federal Register a "notice of the existence and character of the system of records" subject to the Act. Existing notices of systems of records are published biennially in the Federal Register. The Office of the Federal Register compiles and publishes a complete listing of all agencies systems of records in the Register's annual compilation of system notices. A copy of the Department's most recent compilation of systems of records is included in Appendix I. An updated version is provided to appropriate staff immediately after the biennial publication in the Federal Register.

The Privacy Act also requires agencies to send reports to the Congress and the Office of Management and Budget (OMB) on the agency's intention to establish any new system of records and under certain circumstances, the agency's intention to alter an existing system of records. More detailed information describing situations when a report and notice is required is provided in paragraph 4-3 of this handbook. Also, included is guidance on the report and notice content, format, and distribution.

4-2 Responsibilities of the System Manager. The Privacy Act requires that a System Manager be designated for each system of records. More detailed duties are contained in Appendix E. This individual is responsible for:

A. Using the System 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.

B. Establishing the policies, practices, and procedures governing the operation, maintenance, and release of records in the system, including appropriate physical, administrative, and technical safeguards to prevent unauthorized disclosure of information from the system.

C. Establishing procedures and guidelines to ensure that information and data in the system are accurate and necessary; to ensure that an accounting of disclosure is maintained or can be constructed; and to ensure that the routine uses of the

system are compatible with the purposes for which the information was collected.

D. Establishing procedures for access, correction, or amendment of records that conform to the requirements of this chapter and HUD regulations governing the Privacy Act.

E. Ensuring that systems of records notices are kept current and accurate with particular emphasis ensuring that routine use statements are correct and accurate.

F. Preparing drafts of new or altered system reports and related documents and ensuring that systems of records are not operated without first preparing the draft notices and reports and coordinating with the Privacy Act Officer for guidance prior to finalizing the documents.

G. Reviewing routine use statements every 3 years to ensure that the disclosures of records under each routine use are still compatible with the purpose for the system of records.

H. Conducting risk assessments of new or altered systems of records to ensure that appropriate administrative, technical, and physical safeguards are established to protect records in the system from unauthorized disclosure or invasion of privacy.

4-3 Situations Requiring a Report and Federal Register Notice.

A. New and Altered System of Records Report. The Privacy Act requires agencies to publish notices in the Federal Register describing new or altered systems of records, and to submit reports to OMB, and to the Chair of the Committee on Government Operations of the House of Representatives, and the Chair of the Committee on Governmental Affairs of the Senate. See Exhibits 4-1 and 4-2 for examples of a new and an altered System of Records Notice. A notice is also required when an agency conducts a new or altered computer matching program. More specific details relating to this requirement is provided under 5-4. The Privacy Act Officer will work with the system managers to prepare the reports. The reports must be transmitted at least 40 days prior to the operation of the new system of records or the date on which the alteration to an existing system takes place. A new system is one for which no public notice is currently published in the Federal Register. Examples of changes constituting an altered system of records follow:

1. A significant increase in the number of individuals about whom records are maintained. For example, a decision to expand a system that originally covered only residents of public housing in major cities to cover such residents

nationwide would require a report. Increases attributable to normal growth should not be reported.

2. A change that expands the types of categories of information maintained. For example, a file covering single family mortgagors that has been expanded to include multifamily mortgagors would require a report.

3. A change that alters the purpose for which the information is used.

4. A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system. For example, locating interactive terminals at field offices for accessing a system formerly accessible only at Headquarters would require a report.

B. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis or deleting a routine use when there is no longer a need for the disclosure.

C. Exemption Rule. The content of some systems of records may be exempted from the requirement that individuals be permitted access to records through an informal rulemaking process. This process requires publication of a proposed rule, a final rule, and the adoption of the final rule. Agencies may not withhold records under an exemption until these requirements have been met.

4-4 Contents of the New or Altered System Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed Federal Register Notice. There is no prescribed format for either the letter or the narrative statement. The notice must appear in the format prescribed by the Office of the Federal Register's Document Drafting Handbook. Specific requirements relating to the content of the notice are described below. The System Manager will prepare a draft of the system notice and forward it to the Privacy Act Officer to finalize. The Privacy Act Officer will prepare the remaining documentation.

A. Transmittal Letters. The transmittal letter will be signed by the Assistant Secretary for Administration. It should contain the name and telephone number of the individual who can best answer questions about the system of records.

B. Narrative Statement. The narrative statement should be brief.

It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1. Describe the purpose for which the agency is establishing the system of records.

2. Identify the authority under which the system of records is maintained. The underlying programmatic authority for collecting, maintaining, and using the information should be cited. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, cite a general housekeeping statute that authorizes the department to keep such records as necessary.

3. Provide the probable or potential effect of the proposal on the privacy of individuals.

4. Provide a brief description of the steps taken to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established should be available to OMB upon request.

5. Explain how each proposed routine use satisfies the compatibility requirement of subsection (a) (7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine use.

6. Provide OMB Control Numbers, expiration dates, and titles of any OMB approved information collection request (e.g., forms, surveys, etc.) contained in the system of records. If the request for OMB clearance of an information collection is pending, state the title of the collection and the date it was submitted to OMB for clearance.

C. Supporting Documentation. Attach the following to all new or altered system of records reports:

1. A copy of the new or altered system of records notice in Federal Register format. For proposed altered systems a copy of the original system of records notice should be included to ensure that reviewers can understand the changes proposed.

2. A copy of any new exemption rules or changes to published rules that are proposed to issue for the new or altered system.

4-5 Timing, OMB Concurrence, and Publication of the Federal Register Notice.

A. Timing. The Act requires agencies to publish notices in the Federal Register describing new or altered reports 40 days prior to the establishment of a new system of records or prior to the implementation of the amendment to the system of records. Another 40 days should be added to this timeframe to accommodate the time required to prepare the report and obtain appropriate concurrences. All new and altered notices must be routed through the Office of General Counsel, the initiating Office, and the Privacy Act Officer for approval.

B. OMB Concurrence. Approval is assumed, if OMB has not commented within 40 days from the date the transmittal letter was signed. System of records and routine use notices can be published in the Federal Register at the same time that the new or altered system report is sent to OMB and Congress. The period for OMB and congressional review and the notice and comment period for routine uses and exemptions will then run concurrently. Note that exemptions must be published as final rules before they are effective.

C. Notice of Records. The Office of the Federal Register prescribes the format that must be followed for Notices published in the Federal Register. (See the Federal Register Document Drafting Handbook). The Privacy Act requires the publication of specific information concerning systems of records described below:

1. System Name: This is, the name assigned to the system by the Office responsible for the system of records. It should reflect a general description of the contents of the system of records.

2. System location: The address of each location where the system or a portion thereof is maintained is listed here. If the records are maintained in numerous locations, an address directory may be appended to the system or placed at the end of the system notice.

3. Categories of individuals covered by the system: This lists the categories of individuals about whom records are maintained in the system; e.g., "All persons applying for HUD insured mortgages." By reading this heading, an individual should be able to determine if information about him is contained in the system.

4. Categories of Records in the System: This describes the types of records maintained in the system; "individual pay records, individual leave records...." This, too, should help an individual determine if records about him are maintained in the system.

5. Authority for maintenance of the system: This identifies the Federal statute or Presidential Executive Order that authorizes the agency to maintain the system of records. For example, if you are collecting or retrieving information by an individual's social security number (SSN), you must cite the regulation which permits this collection.

6. Routine uses of records maintained in the system, including categories of users and the purposes of such uses: This section must include all the routine uses established for the system. Remember, a routine use is a disclosure outside the agency i.e., HUD maintaining the record for a purpose which is compatible with the purpose for which it was collected. List the entities external to HUD having a need to know the information, e.g., the Internal Revenue Service (IRS), Office of Personnel Management (OPM), the General Accounting Office (GAO), Office of Management and Budget (OMB), etc. Generally, failure to include a particular routine use could prohibit a record from being disclosed without the individual's prior written consent. However, nonconsensual disclosure can be made if some other exception in subsection (b) of the Privacy Act applies.

7. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system: Under this section the following subsections must be listed:

Storage: This describes the methods used to store the records; e.g.,; ...on paper in file folders, on computer tapes...".

Retrievability: This describes what personal identifiers are used to index and retrieve records in the system; e.g., "Records are retrieved by individuals' names and SSN."

Safeguards: Here the measures used to protect the records from unauthorized access or disclosure are listed; e.g. "Records are stored in locked cabinets in rooms to which access is limited to those personnel who service the records."

Retention and disposal: This reveals the length or time the records are maintained and the means of disposal; e.g., "Records are maintained for 15 years after which they are destroyed by shredding.

8. System manager(s) and address: Here is listed the title and complete mailing address of the individual

responsible for implementing the policies and practices regarding the system as outlined in the notice e.g., the Division Director.

9. Notification Procedures: Include the following standard language: "For information, assistance, or inquiry about the existence of records, contact the Privacy Act Officer at the appropriate location, in accordance with procedures in 24 CFR part 16. A list of all locations is given in Appendix B."

10. Contesting record procedures: Include the following standard language: "The Department's rules for contesting the contents of records and appealing initial denials, by the individual concerned, appear in 24 CFR part 16. If additional information or assistance is needed, it may be obtained by contacting: (i) In relation to contesting contents of records, the Privacy Act Officer at the appropriate location (a list of all locations is given in Appendix A) and (ii) in relation to appeals of initial denials, the Department of Housing and Urban Development Departmental Privacy Appeals Officer, Office of General Counsel, Department of Housing and Urban Development, 451 Seventh Street, Southwest, Washington, DC 20410."

11. Record source categories: This describes who, where, or what the information is usually taken from, in general terms (i.e., specific individuals, organizations, or instructions need not be identified), e.g., "Information is obtained from the record subjects, their previous employers, ...

12. Exemptions from Certain Provisions of the Act: If no exemption has been established for the system, indicate "None." If an exemption has been established, state under which provisions of reference (a) it is established (i.e., "Parts of this record system may be exempt under reference (a), subsection (k) (2).").

EXHIBIT 4-1 SAMPLE OF A NEW SYSTEM OF RECORDS NOTICE

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Office of the Secretary

[Docket No.]

Privacy Act of 1974; New System of Records

AGENCY: Department of Housing and Urban Development (HUD)

ACTION: Establish a New System of Records.

SUMMARY: The Department of Housing and Urban Development (HUD) proposes to establish a new record system to add to its inventory of systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

EFFECTIVE DATE: This action will be effective without further notice on (insert date thirty days after date published in the Federal Register) unless comments are received that would result in a contrary determination.

ADDRESSES: Interested persons are invited to submit comments regarding this new system of records to the Rules Docket Clerk, Office of General Counsel, room 10276, Department of Housing and Urban Development, 451 Seventh Street, SW, Washington, DC 20410-0500. Communications should refer to the above docket number and title. An original and four copies of comments should be submitted. Facsimile (FAX) comments are not acceptable. A copy of each communication submitted will be available for public inspection and copying between 7:30 a.m. and 5:30 p.m. weekdays at the above address.

FOR FURTHER INFORMATION CONTACT: Jeanette Smith, Departmental Privacy Act Officer, Telephone Number (202) 708-2374, or William H. Eargle, Director, Office of Finance and Accounting, Telephone Number (202) 708-3310. (These are not toll free numbers.)

SUPPLEMENTARY INFORMATION: Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, notice is given that HUD proposes to establish a new system of records identified as HUD/DEPT- entitled Departmental Accounts entitled Departmental Accounts Receivable Tracking/Collection System (DARTS--D21). Title 5 U.S.C. 552a(e) (4) and (11) provide that the public be afforded a 30-day period in which to comment on the new record system.

The new system report, as required by 5 U.S.C. 552a(r) of the Privacy Act was submitted to the Committee on Governmental Affairs of the United States Senate, the Committee on Government Reform and Oversight of the House of Representatives and the Office of Management Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, dated June 25, 1993 (58 FR 36075, July 2, 1993).

AUTHORITY: 5 U.S.C. 552a

Issued at Washington, DC
Marilynn A. Davis
Assistant Secretary for Administration

HUD/DEPT-

SYSTEM NAME:

Departmental Accounts Receivable Tracking/Collection System (DARTS--D21)

SYSTEM LOCATION:

HUD Computer Center, Lanham, Maryland

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current or former HUD employees or individual participants in HUD programs whose debts to HUD are more than 90 days delinquent.

CATEGORIES OF RECORDS IN THE SYSTEM:

Delinquent debts owed by current or former HUD employees for advances, i.e., travel, payroll, etc., and debts owed by individuals arising from overpayments, audits, court order, et al.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Debt Collection Act of 1982, Pub. L. 97-365.

ROUTINE USES OF RECORDS:

In addition to those disclosures generally permitted under 5 U.S.C. 552 a(b) of the Privacy Act, these records, or information contained therein, may specifically be disclosed outside of the agency as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows, provided that no routine use listed shall be construed to limit or waive any other routine use specified herein:

(a) Internal Revenue Service-- for the purpose of effecting an administrative offset against the debtor for a delinquent debt owed to the U.S. Government by the debtor.

(b) Department of Justice-- for prosecution of fraud, and for the institution of suit or other proceedings to effect collection of claims.

(c) General Accounting Office--for further collection action on any delinquent account when circumstances warrant.

(d) Outside collection agencies and credit bureaus--for the purpose of either adding to a credit history file or obtaining a credit history file on an individual for use in the administration of debt collection for further collection action.

DISCLOSE TO CONSUMER REPORTING AGENCIES:

Disclosure pursuant to 5 U.S.C. 552a(b) (12) may be made from this record system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) or the Federal Claims

Collection Act of 1966 (31 U.S.C. 3701(a) (3). The disclosure is limited to information necessary to establish the identity of the individual, including name, address, and taxpayer identification number (Social Security Number); the amount, status, and history of the claim, and the agency or program under which the claim arose for the sole purpose of allowing the consumer reporting agency to prepare a commercial credit report.

POLICIES AND PRACTICES, FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

Storage: Hard copy files are kept in a locked room, computer records are stored in limited access files in DARTS.

Retrievability: Records are retrieved by social security number (SSN) or name.

Safeguards: These records are available only to those persons whose official duties require such access. Records are kept in limited access areas during duty hours and in locked room at all other times.

RETENTION AND DISPOSAL: As prescribed in the General Records Schedule or for 10 years after debt is paid at a maximum.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Finance and Accounting, 451 7th St S.W., Washington, D.C. 20410.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the particular HUD administrator or component listed in the "system manager" location above.

Individuals should furnish full name, Social Security Number, current address and telephone number.

RECORD ACCESS PROCEDURES: Same as above.

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained from the subjects, Personnel and Payroll systems, HUD's Central Accounting Program System (CAPS), Office of the Inspector General, Office of General Counsel, and other government agencies such as the Department of Justice, General Accounting Office, the Office of Personnel Management, the Departmental Claims Officer (DCO) and documents submitted by various court systems.

EXEMPTIONS FOR CERTAIN PROVISIONS OF THE ACT:

EXHIBIT 4-2 SAMPLE OF AN ALTERED OR AMENDED SYSTEM OF RECORDS NOTICE DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Office of the Secretary [Docket No.]
Privacy Act of 1974; Proposed Amendment to a Systems of Records

AGENCY: Department of Housing and Urban Development (HUD).
ACTION: Notification of a proposed amendment to an existing system of records.
SUMMARY: The Department of Housing and Urban Development (HUD) proposes to amend its system of records entitled "Accounting Records, HUD/DEPT-2" in its inventory of systems of records notices subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. Notice of this system was last published at 55 FR 17676, April 26, 1990.
EFFECTIVE DATE: This action will be effective without further notice on (insert date thirty days after date published in the Federal Register) unless comments are received that would result in a contrary determination.
ADDRESSES: Interested persons are invited to submit comments regarding the proposed amendment to the Rules Docket Clerk, Office of General Counsel, Room 10276, Department of Housing and Urban Development, 451 Seventh Street, SW, Washington, DC 20410-0500. Communications should refer to the above docket number and title. An original and four copies of comments should be submitted. Facsimile (FAX) comments are not acceptable. A copy of each communication submitted will be available for public inspection and copying between 7:30 a.m. and 5:30 p.m. weekdays at the above address. FOR FURTHER INFORMATION CONTACT: Jeanette Smith, Departmental Privacy Act Officer, at (202) 708-2374, or Mary Felton at (202) 708-4256. These are not toll-free numbers.
SUPPLEMENTARY INFORMATION: HUD/DEPT-2 contains a variety of records relating to HUD's accounting functions. These records are maintained for the purpose of supporting HUD's administrative management and collection of delinquent debts, including past due loan payments, overpayments, fines, penalties, fees, damages, interest, leases, sales of real property, that are owed to HUD or to other Federal agencies. Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, notice is given that HUD proposes to modify some of the general routine uses and add new routine uses to this system of records. The revised routine uses (items (i), (k) and (1)) more specifically identify the categories of users (i.e., other Federal agencies) to whom records may be disclosed pursuant to authorized and approved computer matching programs undertaken for debt collection purposes. In addition, HUD is amending other routine uses (items (j), (m), (n), (o), and (p))to permit more effective administrative management and collection of delinquent claims and debts owed to the U.S. Government under any programs administered by HUD.

The amended portion of the system notice is set forth below. Previously, the system and a prefatory statement containing the general routines uses applicable to all HUD systems of records was published in the "Federal Register Privacy Act Issuances, 1989 Compilation, Volume I."

Title 5 U.S.C. 552a(e) (4) and (11) provide that the public be afforded a 30-day period in which to comment on the new record system.

The system report, as required by 5 U.S.C. 552a(r), has been submitted to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget (OMB), pursuant to paragraph 4c of Appendix I to OMB Circular A-130, "Federal Agency Responsibilities for Maintaining Records about Individuals" dated June 25, 1993 (58 FR 36075, July 2, 1993). AUTHORITY: 5 U.S.C. 552a; 88 Stat. 1896; sec 7(d),

Department of HUD Act (42 U.S.C. 3535(d)).
Issued at Washington, D.C._____.
Marilynn A. Davis
Assistant Secretary for Administration

HUD/DEPT-2

System Name: Accounting Records.

Routine uses of Records Maintained in the System, including Categories of Users and the Purpose of Such Uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, other routine uses are as follows:

- **(a): To the U.S. Treasury--for disbursements and adjustments thereof.**
- **(b) To the Internal Revenue Service--for reporting of sales commissions and for reporting of discharged indebtedness;**
- **(c) To the General Accounting Office, General Service Administration, Department of Labor, Labor housing authorities, and taxing authorities--for audit, accounting and financial reference purposes.**
- **(d) To mortgage lenders--for accounting and financial reference purposes, for verifying information provided by new loan applicants and evaluating creditworthiness.**
- **(e) To HUD contractors--for debt and/or mortgage note servicing.**
- **(f) To financial institutions that originated or serviced loans--to give notice of disposition of claims.**
- **(g) To title insurance companies--for payment of liens.**
- **(h) To local recording offices--for filing assignments of legal documents, satisfactions, etc.**
- **(i) To the Defense Manpower Data Center (DMDC) of the Department of Defense and the U.S. Postal Service to conduct computer matching programs for the purpose of identifying and locating individuals who are receiving Federal salaries or benefit payments and are delinquent in their repayment of debts owed to the U.S. Government under certain programs administrated by HUD in order to collect the debts under the provisions of the Debt Collection Act of 1982 (Pub.L. 97-365) by voluntary repayment, or by administrative or salary offset procedures.**
- **(j) To any other Federal agency for the purpose of effecting administrative or salary offset procedures against a person employed by that agency or receiving or eligible to receive**

some benefit payments from the agency when HUD as a creditor has a claim against that person.

(k) With other agencies; such as, Departments of Agriculture, Education and Veteran Affairs, and the Small Business Administration--for use of HUD's Credit Alert Interactive Voice Response System (CAIVRS) to prescreen applicants for loans or loans guaranteed by the Federal Government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Government.

(l) To the Internal Revenue Service by computer matching to obtain the mailing address of a taxpayer for the purpose of locating such taxpayer to collect or to compromise a Federal claim by HUD against the taxpayer pursuant to 26 U.S.C. 6103(m)(2) and in accordance with 31 U.S.C. 3711, 3217, and 3718.

(m) To a credit reporting agency for the purpose of either adding to a credit history file or obtaining a credit history file on an individual for use in the administration of debt collection.

(n) To the U.S. General Accounting Office (GAO), Department of Justice, United States Attorney, or other Federal agencies for further collection action on any delinquent account when circumstances warrant.

(o) To a debt collection agency for the purpose of collection services to recover monies owed to the U.S. Government under certain programs or services administered by HUD.

(p) To any other Federal agency including, but not limited to, the Internal Revenue Service (IRS) pursuant to 31 U.S.C. 3720A, for the purpose of effecting an administrative offset against the debtor for a delinquent debt owed to the U.S. Government by the debtor.

Disclosure to consumer reporting agencies:

Disclosures pursuant to 5 U.S.C 552a(b)(12). Pursuant to 5 U.S.C. 552a(b)(12), disclosures may be made from the record system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) or the Federal Claims Collection Act of 1966, 31 U.S.C. 3701(a) (3)). The disclosure is limited to information necessary to establish the identity of the individual, including name, address and taxpayer identification number (Social Security Number); the amount, status, and history of the claim, and the agency or program under which the claim arose for the sole purpose of allowing the consumer reporting agency to prepare a credit report.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, Disposing of Records in the System and Safeguards:

CHAPTER 5. COMPUTER MATCHING PROGRAMS

5-1 GENERAL. This chapter sets forth procedures for conducting matching programs. The Computer Matching and Privacy Protection Act of 1988 (CMPPA), which amends the Privacy Act, adds certain protection for subjects of Privacy Act records whose records are used in automated matching programs, and regulates the conduct of

computer matching activities. The Act requires HUD to prepare written matching agreements specifying the terms under which matches are to be done.

5-2 DEFINITIONS. All terms defined, in the Privacy Act of 1974 and chapter one of this handbook apply. In addition, the CMPPA provides the following new terms.

A. Matching Program. The comparison of automated records using a computer. Manual comparisons of printouts of two automated data bases are not included in this definition. A matching program covers the actual computerized comparison and any investigative follow-up and ultimate action. Public Law 100-503 divides computer matching programs into covered and non-covered matching programs. Two kinds of matching programs are covered: (1) matches involving Federal benefits programs, and (2) matches using records from Federal personnel or payroll systems of records.

1. Federal Benefit Matches. All four of the following critical elements must be present before a program is covered by the CMPPA. Questions concerning whether a match is covered by the CMPPA should be referred to the Privacy Act Officer.

a. Computerized Comparison of Data. The record comparison must involve records from:

(1) Two or more automated systems of records maintained by Federal agencies that are subject to the Privacy Act; or,

(2) A Federal agency's automated system of records and automated records maintained by a non-Federal agency or agent thereof.

b. Categories of Subjects Covered. The Act covers only the following categories of record subjects:

(1) Applicants (individuals initially applying for benefits) for Federal benefit programs;

(2) Program beneficiaries (individual program participants who are currently receiving or formerly received benefits); and,

(3) Providers of services to support such programs.

c. Types of Programs Covered. Federal benefit programs providing cash or in-kind assistance to individuals.

d. Matching Purpose. The match must have as its purpose one or more of the following:

(1) Establish or verify initial or continuing eligibility for Federal benefit programs;

(2) Verify compliance with the statutory or regulatory requirements of such programs or,

(3) Recoup payments or delinquent debts under such Federal benefit programs.

2. Federal Personnel Matches. Matches comparing records from automated Federal personnel or payroll systems of records, or such records with automated records of State and local governments. Matches in this category must be for other than "routine administrative purposes" as defined in chapter one of this handbook.

3. Excluded matches. A match may meet the criteria established for computer matching, but be excluded if it falls under one of the CMPPA exclusionary clauses. Questions concerning whether a match falls under one of the following exclusions should be referred to the Privacy Act Officer.

a. Statistical matches for which the purpose is solely to produce aggregate data stripped of personal identifiers.

b. Statistical matches for which the purpose is to support a research or statistical project, the data from which may not be used to make decisions that, affect the rights, benefits or privileges of specific individuals.

c. Pilot matches, such as small scale matches to gather benefit/cost data on which to premise a decision about engaging in a full-fledged matching program. A pilot match is forbidden unless it is expressly approved by the Data Integrity Board (DIB) Data developed during a pilot match may not be used to make decisions affecting the rights, benefits, or privileges of specific individuals.

d. Law enforcement investigative matches by an agency or component whose principle statutory function involves the enforcement of criminal laws, the purpose of which is to gather evidence against a named person or persons in an existing investigation. The match must flow from a civil or

criminal law enforcement investigation already underway.

e. Tax administration matches.

f. Routine administrative matches using predominantly Federal personnel records, provided the purpose is not to take any adverse action against Federal personnel, as defined in the Privacy Act.

g. Internal matches using only records from the Department's system of records. However, an internal match whose purpose is to take any adverse financial, personnel, disciplinary or other adverse action against Federal personnel is covered.

h. Background investigations and foreign counterintelligence matches.

B. Recipient Agency. Federal agencies (or their contractors) that receive records from Privacy Act systems of records of other Federal agencies or from State and local governments to be used in matching programs. Recipient agencies are generally assumed to be the beneficiary of a matching program, and are responsible for the reporting and publishing requirements of the Act.

C. Source Agency. A Federal agency that discloses records from a system of records to another Federal agency or to a State or local governmental agency to be used in a matching; or a State or local governmental agency that discloses records to a Federal agency to be used in a matching program. The source agency provides input to HUD in preparing the agreement, and in carrying out the reporting responsibilities, including benefit/cost analysis.

D. Non-Federal Agency. A state or local governmental agency that receives records contained in a system of records from a Federal agency to be used in a matching program. When HUD is a source agency for a match with a non-Federal agency:

1. The program area proposing the match will be responsible for publishing the notice in the Federal Register and reporting the matching to OMB and Congress. The Privacy Act Officer will provide guidance and assistance in preparing the documentation.

2. The non-Federal agency will provide the data needed for HUD to carry out its reporting responsibilities, including benefit/cost analysis.

E. Federal Benefit Program. Any program funded or administered

by the Federal government, or by any agent or State on behalf of the Federal government, that provides cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to U.S. citizens or aliens lawfully admitted for permitted residence.

5-3 The Data Integrity Board (DIB) A Data Integrity Board has been established to provide oversight and review of the department's computer matching agreements. The DIB reviews and approves ongoing matching programs, proposed matches, pilot matches, exclusions, extensions and renewals. HUD's DIB consists of representatives from the major program and administration offices (Office of Housing, Office of Public and Indian Housing, Administration, etc.) of the Department. The only two mandatory members are the Inspector General, who may not serve as Chairperson, and the senior official responsible for the implementation of the Privacy Act, who is the Assistant Secretary for Administration.

5-4 Conducting Matching Programs. HUD staff undertaking matching programs covered by the Act are required to comply with the following requirements.

A. Prior notice to record subjects. Record subjects are to receive either direct or constructive notice that their records may be matched.

1. Direct Notice. By direct notice when there is some form of contact between the government and the subject, e.g., information on the application form when they apply for a benefit or in a notice that arrives with a benefit that they receive;

2. Constructive Notice. By constructive, e.g., publication of Privacy Act systems notices, routine use disclosures, and matching programs in the Federal Register. Constructive notice to record subjects is permissible only when direct notice is not feasible, e.g., emergency situations, certain investigative matches, etc.

B. Federal Register Notices. The CMPPA requires agencies to publish notices in the Federal Register describing new or altered matching programs, and to submit reports to OMB, and to Congress. The report must be received at least 40 days prior to the initiation of any matching activity carried out under a new or substantially altered matching program. For renewals of continuing programs, the report must be dated at least 40 days prior to the expiration of any existing agreement. When the match is approved by the DIBs of all Federal agencies participating, the Privacy Act Officer transmits the notice to the Federal Register, and the report to the Committee on Governmental Affairs of the Senate, the Committee on Government Operations of the House of

Representatives, and OMB. HUD is responsible for publishing the notice if it is the recipient agency or the match is with a non-Federal agency. The Privacy Act Officer will provide guidance on preparing the notice and reports. New or Altered Matching Program Reports should contain the following:

1. Transmittal Letter. The transmittal letter should contain the name and telephone number of the individual who can best answer questions about the matching program. The letter should state that a copy of the matching agreement has been distributed to Congress as the Act requires. The letter to OMB may also include a request for waiver of the review, time period.

2. Narrative Statement. The narrative statement should be brief. It should describe the purpose of the match, provide a description of security safeguards used to protect against any unauthorized access or disclosure of records used in the match, and if the cost/benefit analysis indicated an unfavorable ratio or was waived, an explanation of the basis on which the agency justifies conducting the match.

3. Supporting Documentation. A copy of the Federal Register notice describing the matching program and a copy of the congressional report should be attached.

C. Preparing and Executing Computer Matching Agreements. HUD managers and staff should allow sufficient lead time to ensure that matching agreements can be negotiated and signed in time to secure DIB decisions. For information purposes and for future planning of computer matches see Appendix F, Computer Matching Programs Timetable which shows the estimated time frames related to obtaining internal HUD clearances (program office, Privacy Act Officer, etc.), including specific publication reviews. Federal agencies receiving records from or disclosing records to nonFederal agencies for use in matching programs are responsible for preparing the matching agreements and should solicit relevant data from non-Federal agencies where necessary. Computer matching agreements must contain the following:

1. Purpose and Legal Authority. Since the CMPPA provides no independent authority for the operation of matching programs, HUD staff should cite a specific Federal or State statutory or regulatory basis for undertaking such programs.

2. Justification and Expected Results. An explanation of why computer matching as opposed to some other administrative activity is being proposed and what the

expected results will be.

3. **Records Description. An identification of the Privacy Act systems of records or non-Federal records, the number of records, and what data elements will be included in the match. Projected starting and completion dates for the matching program should also be provided. HUD staff should specifically identify the Federal system or Privacy Act systems of records involved.**

4. **Notice Procedures. A description of the individual and general periodic notice procedures.**

5. **Verification Procedures. A description of the methods HUD will use to independently verify the information obtained through the computer matching program.**

6. **Disposition of Matched Items. A statement that information generated through the match will be destroyed as soon as it has served the matching program's purpose and any legal retention requirements HUD established in conjunction with the National Archives and Records Administration or other cognizant authority.**

7. **Security Procedures. Administrative and technical safeguards to be used in protecting the information will be commensurate with the level of sensitivity of the data and will be fully described.**

8. **Records Usage, Duplication and Redisclosure Restrictions. A description of any specific restrictions imposed by either the source agency or by statute or regulation on collateral uses of the records used in the matching program. The agreement should specify how long a recipient agency may keep records provided for a matching program, and when they will be returned to the source agency or destroyed. In general, recipient agencies should not subsequently disclose records obtained for a matching program and under the terms of a matching agreement for other purposes absent a specific statutory requirement or where the disclosure is essential to the conduct of a matching program.**

9. **Records Accuracy Assessments. Any information relating to the quality of the records to be used in the matching program. Record accuracy is important from two standpoints. In the first case, the worse the quality of the data, the less likely a matching program will have a cost-beneficial result. In the second case, the Privacy Act requires Federal agencies to maintain records they maintain in Privacy Act systems of records to a standard of accuracy that will reasonably assure fairness in any**

determination made on the basis of the record. Thus, an agency receiving records from another Federal agency or from a non-Federal agency needs to know information about the accuracy of such records in order to comply with the law. Moreover, the Privacy Act also requires agencies to take reasonable steps to ensure the accuracy of records that are disclosed to non-Federal recipients.

10. Comptroller General Access. A statement that the Comptroller General may have access to all records of a recipient agency or non-Federal agency necessary to monitor or verify compliance with the agreement. It should be understood that this requirement permits the Comptroller General to inspect State and local records used in matching programs covered by these agreements.

C. Benefit/Analysis The CMPPA requires that a benefit/cost analysis be a part of an agency decision to conduct or participate in a matching program. The intent of this requirement is to ensure that sound management practices are followed when agencies use records from Privacy Act systems of records in matching programs. The DIB may waive the benefit/cost requirement if it determines that such an analysis is not required and the waiver is consistent with OMB guidance. If a matching program is required by statute, the DIB may waive the benefit/cost analysis requirement in its initial review.

5-5 Due Process for Matching Subjects. The CMPPA prescribes certain due process requirements that the subjects of matching programs must be afforded when matches uncover adverse information about them.

A. Verification of Adverse Information. HUD cannot take any adverse action based solely on information produced by a matching program until such information has been independently verified and validated.

B. Notice and Opportunity to Contest. Agencies are required to notify marching subjects of adverse information uncovered and give them an opportunity to explain prior to making a final determination. Generally, individuals are given 30 days to respond to an adverse action, unless a statute grants a longer time.

C. Sanctions. If a record subject can demonstrate that he has been harmed by an agency violation of the CMPPA, the civil remedies of the Privacy Act are available to that record subject.

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.

CHAPTER 7. REPORTING REQUIREMENTS

7-1 INTRODUCTION. In addition to meeting the agency requirements in the Privacy Act, OMB Circular A-130 requires the head of each agency to ensure that the following reviews are conducted as specified below, and be prepared to report the results of such reviews and the corrective action taken to resolve problems uncovered to the Director, OMB. While the Privacy Act Officer will be responsible for performing the reviews and preparing the various reports, input will be required from the administrative and program areas, as needed.

7-2 Examples of Privacy Act Reviews Include:

A. Section (m) Contracts. Every two years review a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his employees.

B. Recordkeeping Practices. Annually review agency recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.

C. Routine Use Disclosures. Every four years review the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.

D. Exemption of Systems of Records. Every four years review each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.

E. Matching Programs. Annually review each ongoing matching program in which the agency has participated during the year, either as a source or as a matching agency, in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.

F. Privacy Act Training. Annually review agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.

G. Violations. Annually review the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem and to find the most effective way to prevent recurrence of the problem.

H. Annually review each system of records notice to ensure that it accurately describes, the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register. See chapter 4 for specific details relating to systems of records requirements.

7-3 Privacy Act Reports. In addition to the above reports, the Privacy Act requires agencies to make the following reports:

A. Biennial Privacy Act Report. This report is submitted to OMB every two years. It includes the number of Privacy Act requests for access to records received during the calendar year, January 1 through December 31. It is important to

remember that only requests for access to records under the Privacy Act should be counted. A request under the Privacy Act is a request which specifies the Privacy Act, or a request which does not specify the Privacy Act but was treated as if it did specify the Act.

B. Biennial Matching Activity Report. The Privacy Act requires agencies to report to OMB every two years on its computer matching activities. At the end of each calendar year the Privacy Act Officer will require each program area that has participated in matches covered by the computer matching provisions of the Privacy Act to submit data summarizing that year's activity. The following data should be included in the report:

1. A listing of the names and positions of the members of the Data Integrity Board and showing separately the name of the Board Secretary, his agency mailing address, and telephone number. Also show and explain any changes in membership or structure occurring during the reporting year.

2. A listing of each matching program, by title and purpose, in which the agency participated during the reporting year. This listing should show names of participant agencies, give a brief description of the program, and give a citation including the date of the Federal Register notice describing the program.

3. For each matching program, an indication of whether the cost/benefit analysis performed resulted in a favorable ratio. The report should explain why the agency proceeded with any matching program for which an unfavorable ratio was reached.

4. For each program which the Board waived a cost/benefit analysis, reasons for the waiver and the results of match, if tabulated.

5. A description of each matching agreement the Board rejected and an explanation of why it was rejected.

6. A listing of any violations of matching agreements that have been alleged or identified, and a discussion of any action taken.

7. A discussion of any litigation involving the agency's participation in any matching program.

8. For any litigation based on allegations of inaccurate records, an explanation of the steps the agency used to ensure the integrity of its data as well as the