City of Manistee Housing Commission
273 6th Avenue • Manistee, Michigan 49660

Phone: (231) 723-6201
Fax: (231) 723-8900
TDD/TTY: (800) 545-1833, ext. 870
manisteehousing@manisteehousing.com

The City of Manistee Housing Commission

Compliance with the

U.S. Privacy Act of 1974 [Amended]

Statement to the Public
February 2016

Executive Summary

The City of Manistee Housing Commission [CMHC1] is a Public Housing Authority under the governance and regulatory requirements of the U.S. Department of Housing and Urban Development [HUD].

The federal National Housing Act of 1934 and the subsequent Housing Act of 1937 established a permanent Public Housing Program providing for States, through legislation, to create local Public Housing Authorities. Michigan Public Act 18 of 1933 authorized the creation of local Public Housing Authorities to be known as Housing Commissions. City of Manistee Ordinance 270 authorized the creation of the City of Manistee Housing Commission and its compliance with State laws and regulations.

HUD, on April 23, 2015 issued Notice PIH 2015-06 "U.S. Department of Housing and Urban Development [HUD] Privacy Guidance for Third Parties." The purpose of the notice is to inform PHAs about their responsibilities for safeguarding personally identifiable information [PII] required by HUD and preventing potential breaches of this sensitive data.

The following Statement of Compliance outlines the requirements set forth by HUD and compliance actions taken by the City of Manistee Housing Commission.

Governing Laws and Regulations

- Section 6 of the Housing Act of 1937
- Privacy Act of 1974 [5 U.S.C. § 552A (Privacy Act)]
- The Freedom of Information Act [FOIA] 5 U.S.C. § 552, and Section 208 of The E-Government Act
- the Housing and Community Development Act of 1987
- 42 U.S.C. § 1437d (q)(4)
- 42 U.S.C. § 1437d (t)(2)
- 42 U.S.C. § 3543
- the Stewart B. McKinney Homeless Assistance Act of 1988
- 42 U.S.C. § 3544
- 24 C.F.R Part 5, Subpart B
- 42 U.S.C. 3544(c)(2)(A)
- 26 U.S.C. 6103(l)(7)(C)
- 24 C.F.R. 5.212
- Federal Acquisition Regulation (FAR), 48 C.F.R. 24.104, clause 52.224-2

Additional Federal Guidance

- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB M-04-26, Personal Use Policies and —File Sharing Technology
- OMB M-05-08, Designation of Senior Agency Officials for Privacy
- OMB M-06-15, Safeguarding Personally Identifiable Information
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (FISMA). FISMA requires federal agencies to implement a mandatory set of processes designed to ensure the confidentiality, integrity, and availability of system related information. FISMA requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner.

Definitions

- *Personally Identifiable Information (PII).* Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
- *Sensitive Personally Identifiable Information.* PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

CMHC Management of Personally Identifiable Information [PII] and Sensitive Identifiable Information [SPII]

CMHC Compliance Management of PII

The CMHC is required, by the above referenced laws and regulations, and specifically Notice PIH 2015-06 "U.S. Department of Housing and Urban Development [HUD] Privacy Guidance for Third Parties" to protect the PII and SPII of public housing program participants. The CMHC shall, at minimum, take the following actions to protect the PII and SPII of public housing program participants.

The definition of PII includes the individual's name and other information that is linked or linkable to a specific individual, therefore CMHC shall

- Maintain all printed records containing PII in a secure room using a limited access, non-duplicative lock and key system other than when in use by authorized CMHC staff for authorized purposes
- Maintain a high level of electronic security on its computers, servers, internet connections, electronic communication devices and electronic storage and transfer systems
- Redact all PII from any documents made available to the public
- Not admit or deny the residence of any public housing program participant, including head of household, co-head and members of the family to any person other than the individual and/or his/her legal representative [upon verification of legal representative status] and except for authorized individuals and/or agencies permitted by federal law [e.g. the IRS, law enforcement, the Census Bureau, etc.]
- Withhold all PII from individuals, agencies, representatives, etc. unless a written authorization of release of information is presented executed by the head of household or co-head or his/her legal representative [and only upon verification of the documentation presented]
- Take all such action as deemed necessary to protect the PII of public housing program participants

CMHC Compliance Management of SPII

In addition to the actions outlined above to protect PII, in order to safeguard and protect SPII CMHC shall take, at minimum, the following actions:

- Share or discuss SPII only with those personnel who have a need to know for the purpose of their work. Challenge anyone who asks for access to SPII for which the PHA is responsible
- Prohibit the distribution or release SPII to other employees, contractors, or other third parties unless convinced that the release is authorized, proper and necessary
- When discussing SPII on the telephone, confirm that the person being spoken to is the right person before discussing the information and inform him/her that the discussion will include SPII
- Never leave messages containing SPII on voicemail
- Never send SPII electronically via email
- Avoid discussing SPII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations
- Hold meetings in a secure space [i.e., no unauthorized access or eavesdropping possible] if SPII will be discussed and ensure that the room is secured after the meeting
- Treat notes and minutes from such meetings as confidential unless it can be verified that they do not contain SPII

Conclusion

The City of Manistee Housing Commission takes the protection of all personally identifying information of Public Housing program participants seriously and shall comply with all laws and regulations ensuring the protection of such information of program participants. Questions concerning CMHC's compliance with the Privacy Act are to be directed to either the CMHC Executive Director or General Counsel.

List of Attachments

- Notice PIH 2015-06
- HUD Privacy Act Rules of Conduct
- HUD Privacy Principles
- HUD Privacy Act Handbook

U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

SPECIAL ATTENTION OF:
Directors of HUD Regional and Field Offices of Public Housing;
Public Housing Agencies that Receive Funds under Any Public and Indian Housing Program

NOTICE PIH-2015-06

Issued: April 23, 2015

Expires: Effective until amended, superseded, or rescinded

Cross References:
PIH 2014-10, PIH 2010-15

Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection Guidance for Third Parties

1) **Purpose**: This notice informs all public housing agencies (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

   PIH 2014-14 is being revised to include guidance to assist PHA system administrators and users to fulfill their requirements for information technology security awareness training.

2) **Background**: Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d (q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.

   a) General HUD program requirements are set forth in 24 C.F.R. Part 5, Subpart B, Disclosure and Verification of Social Security Numbers and Employer Identification Numbers: Procedures for Obtaining Income Information. Subpart B enables HUD and

PHAs to obtain income information about applicants and participants in the covered programs through computer matches with State Wage Information Collection Agencies (SWICAs) and Federal agencies, in order to verify an applicant's or participant's eligibility for or level of assistance.

i) *Restrictions on Use of Income Information Obtained from SWICA and Federal Agencies.* The restrictions of 42 U.S.C. 3544(c)(2)(A) apply to the use by HUD or a PHA of income information obtained from a SWICA and the restrictions of 42 U.S.C. 3544(c)(2)(A) and of 26 U.S.C. 6103(l)(7)(C) apply to the use by HUD or a PHA of income information obtained from the Internal Revenue Service or the Social Security Administration.

b) The Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. 5.212 which states:

i) *Compliance with the Privacy Act*. The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

Privacy Act Notice. All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

c) The Federal Acquisition Regulation (FAR), 48 C.F.R. 24.104, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:

(a) The Contractor agrees to—
(1) *Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ….*

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

d) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:

i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy

ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

iii) OMB M-04-26, Personal Use Policies and ―File Sharing Technology

iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy

v) OMB M-06-15, Safeguarding Personally Identifiable Information

vi) OMB M-06-16, Protection of Sensitive Agency Information

vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance

ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

x) OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (FISMA). FISMA requires federal agencies to implement a mandatory set of processes designed to ensure the confidentiality, integrity, and availability of system related information. FISMA requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner.

e) Definitions

As used in this Notice, the following terms are defined as:

i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

3) **Guidance on Protecting Sensitive Privacy Information**: The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate

administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

a) Contractors and third party business partners should take the following steps to help ensure compliance with federal requirements:

i) Security Awareness and Privacy Training

(1) The National Institute of Standards and Technology (NIST) publishes templates and guides for what security awareness trainings should entail in order to be FISMA compliant. These guidelines focus on the following key aspects:

- **Confidentiality** - Protecting information from unauthorized access and disclosure.
- **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
- **Availability** - Defending information systems and resources to ensure timely and reliable access and use of information. As such, systems are vulnerable to misuse, interruptions and manipulation.
- **Threat**- A threat in the case of IT security is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of protected information.
- **Vulnerability**- Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy
- **Risk** is the likelihood that a threat will exploit vulnerability.
- **Controls** are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability

(2) Additionally, the NIST provides publications for reference on Building an Information Technology Security Awareness and Training Program and Security and Privacy Controls for Federal Information Systems and Organizations

(3) PHAs should maintain adequate documentation that supports the training for all staff as well as maintain auditable records of training completion. Although there is not required reporting on the training, Office of Field Operations personnel may spot-check compliance on on-site visits.

ii) Limit Collection of PII

(1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

(2) Consistent with the provisions of this Notice, PHAs may enter into agreements (or in some cases be required) to provide PII to legitimate researchers under contract

or other agreement with HUD to support studies on the effects and operations of HUD programs. Further, HUD encourages PHAs to supply PII to other legitimate researchers who do not have contracts or other agreements with HUD in support of such studies, so long as the PHA in question has taken reasonable precautions to prevent disclosure of PII outside of the research team. Such reasonable precautions generally involve written agreements between the PHA and one or more researchers that specify the legal obligations of the latter to protect PII from disclosure.

iii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iv) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include ―For Official Use Only or ―For (Name of Individual/Program Office) Use Only.

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

v) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

vi) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement ―To Be Opened By Addressee Only.

vii) Records Management, Retention, and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

viii) Incident Response

(1) Supervisors should ensure that all personnel are familiar with reporting procedures.

(2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

ix) Contact Information

Inquiries about this notice should be directed to Matthew Steen, Privacy Liaison Officer, Real Estate Assessment Center, Office of Public and Indian Housing, at 202-475-8933.

x) **Paperwork Reduction Act**. The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, HUD may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a currently valid OMB control number.

/s/

Lourdes Castro Ramírez,
Principal Deputy Assistant Secretary for
Public and Indian Housing

U.S. Department of Housing and Urban Development
Privacy Act Rules of Conduct

The Privacy Act of 1974 (5 U.S.C. 552a), requires the establishment of "rules of conduct" for all persons involved in the design, development, operation, and maintenance of a Privacy Act system of records, and the penalties for non-compliance.

All HUD employees and contractors have an obligation to safeguard information under the provisions of the Privacy Act. Consequently, all HUD employees and contractors shall:

- Ensure that personal information contained in system of records, to which they have access or are using to the conduct of official business, shall be protected so that the security and confidentially of the information shall be preserved.

- Not disclose any personal information contained in any system of records except as authorized.

- Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to the HUD HITS NATIONAL Help desk.

- Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities for protecting personal information being collected and maintained under HUD's Privacy Program.

- Prepare promptly any required new, amended, or altered systems notices for the system of records and submit them thought HUD's Privacy Officer for publication in the Federal Register.

- Not maintain any official files on individuals that are retrieved by name or other personal identifier without first ensuring that a notice of the system of records has been published in the Federal Register.

- Minimize the collection of data containing personal information.

HUD employees and contractors who willfully disclose personal information when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administration sanctions. Any official, who willfully maintains a system of records without meeting the publication requirement of the Act, is subject to possible criminal penalties and/or administrative sanctions. The Privacy Act of 1974 provides misdemeanor criminal charges and a fine of up to 5,000 for anyone who knowing and willfully violates the Privacy Act.

Privacy Principles

The privacy principles set forth in this document are based on the ethical and legal obligations of the Department to all employees, business partners, and clients. The obligation to protect privacy and to safeguard the information individuals entrust to HUD is a fundamental part of HUD?s mission to administer its programs fairly and efficiently. Individuals have the right to expect that the information they provide will be safeguarded and used only in accordance with law.

All HUD employees are required to conduct their actions in a way that reflects a commitment to deal with individuals fairly and honestly, and to protect their right to privacy by ensuring that their personal information is protected. To promote and maintain individuals? trust in privacy, confidentiality and security protections provided by HUD, the Department will be guided by the following privacy principles:

- Protecting individual privacy and safeguarding confidential information are a public trust
- No information will be collected or used that is not necessary and relevant for the administration of HUD?s programs, and other legally mandated or authorized purposes.
- Information will be collected, to the greatest extent practicable, directly from the individual to whom it relates.
- Information about individuals collected from third parties will be verified to the greatest extent practicable with the individuals themselves before any adverse action is taken against them.
- Personally identifiable information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
- Personally identifiable information will be disposed of at the end of the retention period required by law or regulation.
- Individual information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside of HUD other than as authorized by law and in the performance of official duties.
- Unauthorized access to individual information by any HUD employee constitutes a serious breach of the confidentiality of that information and will not be tolerated.
- Requirements governing the accuracy, reliability, completeness, and timeliness of individual information will ensure fair treatment of all individuals.
- The privacy rights of individuals will be respected at all times and every individual will be treated honestly, fairly, and respectfully.

Related Information

Privacy Impact Assessments
Your Rights to Federal Records
Policies, Procedures and Guidelines
HUD Systems of Records Notices

Privacy Act Handbook

Directive Number: 1325.1

U.S. Department of Housing and Urban Development
Office of Administration

SPECIAL ATTENTION OF: TRANSMITTAL
Handbook No.: 1325.01 REV-01
ISSUED: September 1, 1995

1. This Transmits Handbook 1325.01 REV-01, Privacy Act Handbook.

2. Summary. The entire handbook has been revised to clarify the policies, procedures, and guidelines for the implementation of the Department's Privacy Act Program and to incorporate new OMB Circular A-130 requirements. It should be read in its entirety.

3. Filing Instructions

Remove	Insert
Handbook 1325.1 dated 10/76	Revised Handbook 1325.1 REV-1

AMII: Distribution: W-3-1,W-1,W-3,R-1,R-2,R-6,R-7,R-8

U.S. Department of Housing and Urban Development
Office of Administration

SPECIAL ATTENTION OF: TRANSMITTAL

Handbook No: 1325.01 CHG-5
Issued: August, 1993

---

1. This Transmits Handbook 1325.01 CHG-5, Privacy Act Handbook.

2. Summary. CHG-5 provides information concerning the policies and procedures to be followed when implementing a computer matching program.

   Background. Notice 91-0012 ADM issued October 22, 1991 and due to expire on October 30, 1993, provided highlights of the Computer Matching and Privacy Protection Act. That Notice is being incorporated herewith as Chapter 6 to the Privacy Act Handbook.

3. Filing Instructionsi

Remove	Insert
Table of Contents	Table of Contents

Pgs. i, ii, iii	Pgs. i, ii, iii, dated 8/93
	Pgs. 6-1 to 6-5, dated 8/93
	Appendices 7 and 8, dated 8/93

AII : Distribution : W-3-1, W-1, W-3, R-1, R-2, R-6, R-7, R-8.

W-3-1, W-1, W-3, R-1, R-2, R-6, R-7, R-8
W-3-1 Directives Management Officers--Headquarters and Regions, library, ACIR (Advisory Commission on Intergovermental Relations)
W-1 Assistant Secretaries, Deputy Assistant Secretaries, General Counsel, staff offices reporting to the Secretaryi
W-3 HQ Division Directors, those reporting directly to Office Directors, multiple copies for staff
R-1 Regional Administrators, Deputy Regional Administrators
R-2 Office Directors, Principal Assistants in Regional Administrators' offices
R-6 Category A offices - Office Managers and Deputy Office Managers
R-7 Category B offices - Office Managers and Deputy Office Managers
R-8 Category C offices - Office Managers and Deputy Office Managers

---

Special Attention of: Transmittal Handbook No. 1325.1 CHG-4

Regional Administrators Issued: March 1984
Area Office Managers
Service Office Supervisors

1. This Transmitsi

Changes to Handbook 1325.1, Privacy Act Handbook.

2. Explanation of changes:

These changes clarify the criteria for identifying Privacy Act systems of records; highlight the more significant responsibilities of Privacy Act system managers (Appendix 5); provide guidelines for establishing safeguards for records subject to the Privacy act (Appendix 6); and reflect current organizational structures. Chapter 5 has been added to describe Privacy Act reporting requirements.

3. Filing instructions:

Remove:	Insert:
Pages i, ii, and iii	Pages i, ii, and iii dated 3/84
Pages 1-1 through 1-6	Pages 1-1 through 1-7 dated 3/84
Pages 2-3 and 2-4	Pages 2-3 and 2-4 dated 3/84a

Pages 3-1 and 3-2	Pages 3-1, 3-2, and 3-2.1 dated 3/84
Pages 3-41 through 3-45	Pages 3-41 through 3-46 dated 3/84
Pages 4-1 through 4-4	Pages 4-1 through 4-4 dated 3/84
Pages 5-1 and 5-2	Pages 5-1 and 5-2 dated 3/84
	Appendix 5, pages 1 through 3 dated 3/84
	Appendix 6, pages 1 and 2 dated 3/84

U. S. Department of Housing and Urban Development
ADMINISTRATION

Special Attention of: Transmittal Handbook No. 1325.l CHG-3

Issued: November 19, 1981i

Regional Administrators
Area Office Managers
Service Office Supervisors

1. This Transmits changes to Handbook 1325.1, Privacy Act Handbook.

2. Explanation of changes:
These changes contain reporting requirements for information which must be sent to Headquarters by no later than January 25 of each year. They also contain an updated table of contents.

3. Filing instructions:

Remove:	Insert:
Pages i and ii dated 10/76	Pages i dated 10/76 and ii CHG-3 dated 11/81
Page iii dated 10/76	Page iii CHG-3 dated 11/81
	Chapter 5, Reporting Requirements, dated 11/81.i

U. S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

TRANSMITTAL 1325.1 CHG-2

1. This transmits:

Changes to Handbook 1325.1, Privacy Act Handbook.

2. Explanation of changes:

These changes delete references to the Civil Service Commission and replace them with references to the Office of Personnel Management.

3. Filing instructions:

Remove:	Insert:i
Pages 1-1 dated 10/76 and 1-2 CHG-1 dated 1/8/81	Pages 1-1 CHG-2 dated 7/81 and 1-2 CHG-1 dated 1/81
Pages 3-23 dated 10/76 and 3-24 dated 10/76	Pages 3-23 CHG-2 dated 7/81 and 3-24 dated 10/76
Pages 3-25 and 3-26 dated 10/76	Pages 3-25 dated 10/76 and 3-26 CHG-2 dated 7/81
Pages 1 and 2 Appendix 4 dated 10/76	Page 1 Appendix 4 dated 10/76 and page 2 CHG-2 Appendix 4 dated 7/81.

U. S. Department of Housing and Urban Development
ADMINISTRATION

TRANSMITTAL 1325.1 CHG-1

January 14, 1981i

1. This transmits:

Changes to Handbook 1325.1, Privacy Act Handbook.

2. Explanation of changes:

These changes clarify the role of the Departmental Privacy Act Officer; change office titles to comply with current practices; describe the responsibilities of Privacy Act Coordinators; clarify the responsibilities of Privacy Act System Managers; delete Appendix 3 containing a reprint of 24 CFR 16 (a copy of Departmental Rules and Regulations concerning the Privacy Act); reserve Appendix 3 until 24 CFR 16 is revised and published; clarify that the Assistant Secretary for Administration, rather than the Secretary, submits the report of a new/altered system to Congress and the Office of Management and Budget, and publishes the notice of existence and character of the systems of records; update the list of contents of the Privacy Act system notice; add the requirement that any Advanced Requirements Notice involving a computer matching program be cleared by the Departmental Privacy Act Officer; delete reference to a Departmental Privacy Act Committee; delete reference to the Privacy Protection Study Commission; and state ai more realistic time frame for obtaining internal Departmental clearance of Privacy Act system notices.

3. Filing instructions:

Remove:	Insert:
Pages 1-1 and 1-2 dated 10/76	Pages 1-1 dated 10/76, 1-2 CHG-1 dated 1/81 and 1-2.1 CHG-1 dated 1/81.
Pages 3-11 and 3-12 dated 10/76	Pages 3-11 dated 10/76, 3-12 CHG-1

dated 1/81.

Remove:	Insert:
Pages 3-13 and 3-14 dated 10/76	Pages 3-13 CHG-1 dated 1/81, 3-14 CHG-1 dated 1/81, and 3-14.1 CHG-1 dated 1/81.
Pages 3-39 and 3-40 dated 10/76	Pages 3-39 CHG-1 dated 1/81, 3-40 CHG-1 dated 1/81 and 3-40.1 CHG-1 dated 1/81.
Pages 3-41 and 3-42 dated 10/76	Pages 3-41 CHG-1 dated 1/81, 3-41.1 CHG-1 dated 1/81, and 3-42 CHG-1 dated 1/81.
Pages 3-43 and 3-44 dated 10/76	Pages 3-43 CHG-1 dated 1/81, and 3-44 CHG-1 dated 1/81.
Pages 3-45 and 3-46 dated 10/76	Pages 3-45 dated 10/76 and 3-46 CHG-1 dated 1/81.
Pages 4-1 and 4-2 dated 10/76	Pages 4-1 CHG-1 dated 1/81 and 4-2 dated 10/76.
Pages 4-3 and 4-4 dated 10/76	Pages 4-3 CHG-1 dated 1/81 and 4-4 dated 10/76.
Appendix 1, Pages 15, 16 and 17 dated 10/76	Appendix 1, Pages 15 dated 10/76 16 CHG-1 dated 1/81 and 17 CHG-1 dated 1/81.
Appendix 3, Pages 1 through 12 dated 10/76	Appendix 3, Page 1 CHG-1 dated 1/81.

1/81

Transmittal 1325.1

October 27, 1976

1. This Transmits:
   Handbook 1325.1, Privacy Act Handbook.

2. Purpose:

   a. To provide every employee of the Department with information on their rights and responsibilities under the Privacy Act of 1974.

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

3. Filing Instructions:

Insert Handbook 1325.1

W-1, W-2, W-3, W-3-1, R-1, R-2, R-4, R-5

W-1	Assistant Secretaries, Deputy Assistant Secretaries, General Counsel, staff offices reporting to the Secretary
W-2	HQ Office Directors, Special Assistants, those reporting directly to Assistant Secretaries
W-3	HQ Division Directors, those reporting directly to Office Directors, multiple copies for staff
W-3-1	Directives Management Officers--Headquarters and Regions, library, ACIR (Advisory Commission on Intergovermental Relations)
R-1	Regional Administrators, Deputy Regional Administrators
R-2	Office Directors, Principal Assistants in Regional Administrators' offices

[Search] [Prev List] [Doc List] [Next List] [First Doc] [Prev Doc] [Curr Doc] [Next Doc] [Last Doc] [Top] [Help]

TABLE OF CONTENTS

Appendices

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.

Title and Description of Record:

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 Action	Name of Person Contacted	Location of Person Contacted	Type of Action 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:

None.

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 verification process it used in the matching program, including an assessment of the adequacy of each.

C. New and Altered System of Records Report. The 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 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. The specific requirements pertaining to the report are found in paragraph 4-3 of this handbook.

D. New or Altered Matching Program Report. The Act 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 specific requirements pertaining to the report are found in Chapter 5 of this handbook.

Appendix A

Privacy Act Case Log
US Department of Housing and Urban Development

	Case Num./Name	Case Num./Name	Case Num./Name	Case Num./Name	Case Num./Name	Case Num./Name
Action Requested						
Date request received						
Date request Transferred						
10-day extension notice sent						
Request for additional Information sent						
Request for additional information received						
Official Processing Date						
Departmental Action Type and Date						
Date Requester Appeal Upheld						
Departmental Action taken In response to appeal and date						
Information sent to requester						
Information sent to Other agencies						
Comments						

Appendix B -- Privacy Act Officers' Locations

NEW ENGLAND FIELD OFFICES
(Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont)

CONNECTICUT STATE OFFICE
Connecticut State Coordinator
330 Main Street, First Floor
Hartford, CT 06106-1860
Telephone Number: 203-240-4522
Facsimile Number: 203-240-4674

MAINE STATE OFFICE
Maine State Coordinator
First Floor
99 Franklin Street
Bangor, ME 04401-4925
Telephone Number: 207-945-0467
Facsimile Number: 207-945-0533

MASSACHUSETTS STATE OFFICE
Secretary's Representative
Thomas P. O'Neil, Jr. Federal Building
10 Causeway Street, Room 375
Boston, MA 02222-1092
Telephone Number: 617-565-5234
Facsimile Number: 617-565-5166

NEW HAMPSHIRE STATE OFFICE
New Hampshire State Coordinator
Norris Cotton Federal Building
275 Chestnut Street
Manchester, NH 03101-2467
Telephone Number: 603-666-7681
Facsimile Number: 603-666-7736

RHODE ISLAND STATE OFFICE
Rhode Island State Coordinator
Sixth Floor
10 Waybosset Street
Providence, RI 02903-3234
Telephone Number: 401-528-5351
Facsimile Number: 401-528-5312

VERMONT STATE OFFICE
Coordinator,
Vermont State Coordinator,
U.S Federal Building, Room 244
11 Elmwood Avenue
P.O. Box 879
Burlington, VT 05402-0879-5312
Telephone Number: 802-951-6290
Facsimile Number: 802-951-6298

ALBANY AREA OFFICE
Albany Area Coordinator,
52 Corporate Circle
Albany, NY 12203-5121
Telephone Number: 518-464-4200
Facsimile Number: 518-464-4300

BUFFALO AREA OFFICE
Buffalo Area Coordinator,
Lafayette Court
465 Main Street, Fifth Floor
Buffalo, NY 14203-1760
Telephone Number: 716-551-5755
Facsimile Number: 716-846-5752

CAMDEN AREA OFFICE
Camden Area Coordinator,
Hudson Building
600 Hudson Square, Second Floor
Camden, NJ 06102-1156
Telephone Number: 609-757-5081
Facsimile Number: 609-757-5373

NEW JERSEY STATE OFFICE
New Jersey State Coordinator,
One Newark Center
13th Floor
Newark NJ 07102-5260
Telephone Number: 201-622-7900
Facsimile Number: 201-645-6239

MID ATLANTIC FIELD OFFICES
(Delaware, District of Columbia, Maryland, Pennsylvania, Pittsburgh, Virginia, West Virginia)

DELAWARE STATE OFFICE
Delaware State Coordinator,
824 Market Street, Suite 850
Wilmington, DE 19601-3016
Telephone Number: 302-573-6300
Facsimile Number: 302-573-6259

DISTRICT OF COLUMBIA OFFICE
District of Columbia

820 First Street, N.E.
Washington, DC 20002-4205
Telephone Number: 202-275-9200
Facsimile Number: 202-275-0779

MARYLAND STATE OFFICE
Maryland State Coordinator,

NEW YORK/NEW JERSEY FIELD OFFICES
(New York, New Jersey, Albany, Buffalo, Camden)

NEW YORK STATE OFFICE
Secretary's Representative
26 Federal Plaza
New York NY 10278-0068
Telephone Number: 212-264-6500
Facsimile Number: 212-264-0246

PENNSYLVANIA STATE OFFICE
Secretary's Representative
Coordinator,
The Wanamaker Building
100 Penn Square East
Philadelphia PA 19107-3380
Telephone Number: 215-656-0600
Facsimile Number: 215-656-3433

VIRGINIA STATE OFFICE
Virginia State Coordinator,
The 3600 Centre
3600 West Broad Street
P.O. Box 90331
Richmond, VA 23230-0331
Telephone Number: 804-278-4507
Facsimile Number: 804-278-4516

WEST VIRGINIA STATE OFFICE
West Virginia State Coordinator,
Kanawha Valley Building
405 Capitol Street, Suite 708
Charleston,WV 25301-1795
Telephone Number: 304-347-7000
Facsimile Number: 304-347

SOUTHEAST/CARIBBEAN FIELD OFFICES
(Georgia, Alabama, Florida, South Carolina, North Carolina, Mississippi, Memphis, Tampa, Orlando, Knoxville, Jacksonville, Kentucky, Coral Gables, Caribbean)

GEORGIA STATE OFFICE
Secretary's Representative
Richard B. Russell Federal Building
75 Spring Street, S.W.
Atlanta, GA 30303-3388
Telephone Number: 404-331-5136
Facsimile Number: 404-331-0845

ALABAMA STATE OFFICE
Alabama State Coordinator
Annex
City Crescent Building
10 South Howard Street, Fifth Floor
Baltimore, MD 21201-2505
Telephone Number: 410-962-2520
Facsimile Number: 410-962-4947

NORTH CAROLINA STATE OFFICE
North Carolina State

Koger Building
2306 West Meadowview Road
Greensboro NC 27407-3707
Telephone Number: 910-547-4000
Facsimile Number: 910-547-4015

MISSISSIPPI STATE OFFICE
Mississippi State Coordinator,
Doctor A. H. McCoy Federal Building
100 West Capitol Street, Room 910
Jackson, MS 39288-1016
Telephone Number: 601-965-5308
Facsimile Number: 601-965-4773

MEMPHIS AREA OFFICE
Memphis Area Coordinator,
One Memphis Pace
200 Jefferson Avenue, Suite 1200
Memphis, TN 38103-2335
Telephone Number: 901-544-3367
Facsimile Number: 901-544-3697

TENNESSEE STATE OFFICE
Tennessee State Coordinator,
251 Cumberland Bend Drive, Suite 200
Nashville, TN 37228-1803
Telephone Number: 615-736-5213
Facsimile Number: 615-736-2018

PITTSBURGH AREA OFFICE
Pittsburgh Area Coordinator,
412 Old Post Office Courthouse Bldg.
7th and Grant Street
Pittsburgh, PA 15219-1906
Telephone Number: 412-644-6428
Facsimile Number: 412-644-6499

TAMPA AREA OFFICE
Tampa Area Coordinator,
Timberlake Federal Building

Beacon Ridge Tower
600 Beacon Parkway West, Suite 300
Birmingham, AL 35209-3144
Telephone Number: 205-290-7617
Facsimile Number: 205-290-7593

FLORIDA STATE OFFICE
Florida State Coordinator
8600 Northwest 36th Street, Suite 3100
270 P.O. Box 4622
Miami, FL 33166-4022
Telephone Number: 305-717-2500
Facsimile Number: 305-717-2515

SOUTH CAROLINA STATE OFFICE
South Carolina State Coordinator
Strom Thurmond Federal Building
1835 Assembly Street
Columbia, SC 28201-2460
Telephone Number: 603-765-5592
Facsimile Number: 603-765-5515

501 East Polk Street, Suite 700
Tampa, FL 33602-3945
Telephone Number: 813-228-2501
Facsimile Number: 813-228-2431

ORLANDO AREA OFFICE
Orlando Area Coordinator,
Langley Building
3751 Maguire Boulevard, Suite
Orlando, FL 32803-3032
Telephone Number: 407-648-6441
Facsimile Number: 407-648-6310

KNOXVILLE AREA OFFICE
Knoxville Area Coordinator,
John J. Duncan Federal Building
710 Locust Street, Third Floor
Knoxville, TN 37902-2526
Telephone Number: 615-545-4384
Facsimile Number: 615-545-4569

JACKSONVILLE AREA OFFICE
Jacksonville Area Coordinator
Southern Bell Tower
301 West Bay Street, Suite 2200
900
Jacksonville, FL 32202-5121
Telephone Number: 904-232-2626
Facsimile Number: 904-232-3759

KENTUCKY STATE OFFICE
Kentucky State Coordinator
601 West Broadway
Post Office Box 1044
Louisville, KY 40201-1044
Telephone Number: 502-582-5251
Facsimile Number: 502-582-6074

CORAL GABLES AREA OFFICE
Coral Gables Area Coordinator
Gables 1 Tower
1320 South Dixie Highway
Coral Gables, FL 33146-2911
Telephone Number: 305-662-4500
Facsimile Number: 305-662-4519

CARIBBEAN OFFICE
Caribbean Coordinator
New San Juan Office Building
159 Carlos E. Chardon Avenue
San Juan, PR 00918-1804
Telephone Number: 809-766-6121
Facsimile Number: 809-766-5995

ARKANSAS STATE OFFICE
Arkansas State Coordinator,
TCBY Tower
425 West Capitol Avenue, Suite

Little Rock, AR 72201-3488
Commercial Number: 501-324-5931
Facsimile Number: 501-324-5900

LUBBOCK AREA OFFICE
Lubbock Area Coordinator,
George H. Mahon Federal Building
and United States Courthouse
1205 Texas Avenue
Lubbock, TX 79401-4093
Telephone Number: 806-743-7265
Facsimile Number: 806-743-7275

LOUISIANA STATE OFFICE
Louisiana State Coordinator,
Ninth Floor
Hale Boggs Federal Bldg.
501 Magazine Street
New Orleans, LA 70130-3099
Telephone Number: 504-589-7200
Facsimile Number: 504-589-2917

OKLAHOMA STATE OFFICE
Oklahoma State Coordinator,
500 Main Plaza
500 West Main Street, Suite 400
Oklahoma City, OK 73102-3202

Telephone Number: 405-553-7400
Facsimile Number: 405-553-
0196

SOUTHWEST FIELD OFFICE
Texas, New Mexico, Dallas, Houston, Arkansas, Lubbock, Louisiana, Oklahoma, San Antonio, Shreveport, Tulsa)

TEXAS STATE OFFICE
Secretary's Representative
1600 Throckmorton
Post Office Box 2905
Fort Worth, TX 76113-2905
Telephone Number: 817-885-5401
Facsimile Number: 817-885-5629

NEW MEXICO STATE OFFICE
New Mexico State Coordinator
625 Truman Street, N.E.
Albuquerque, NM 87110-6443
Telephone Number: 505-262-6463
Facsimile Number: 505-262-6604

DALLAS AREA OFFICE
Dallas Area Coordinator
525 Griffin Street, Room 860
Dallas, TX 75202-5007
Telephone Number: 214-767-8359
Facsimile Number: 214-767-8973

HOUSTON AREA OFFICE
Houston Area Coordinator
Norfolk Tower
2211 Norfolk, Suite 200
Houston,TX 77098-4096
Telephone Number: 713-834-3274
Facsimile Number: 713-834-3319

SAN ANTONIO AREA OFFICE
San Antonio Area Coordinator,
Washington Square
600 Dolorosa Street
San Antonio, TX 78207-4563
Telephone Number: 210-229-6800
Facsimile Number: 210-229-6804

SHREVEPORT AREA OFFICE
Shreveport Area Coordinator,
401 Edwards Street, Suite 1510
Shreveport, LA 71101-3107
Telephone Number: 318-676-3385
Facsimile Number: 318-676-3407

TULSA AREA OFFICE
Tulsa Area Coordinator,
50 East 15th Street
Tulsa, OK 74119-4030
Telephone Number: 918-581-7434
Facsimile Number: 918-581-7440

MIDWEST FIELD OFFICES
(Cincinnati, Cleveland, Flint, Grand Rapids, Illinois, Indiana, Michigan, Minnesota, Ohio, Springfield, Wisconsin)

CINCINNATI AREA OFFICE
Cincinnati Area Coordinator
525 Vine Street
Cincinnati, OH 45202-3188
206
Telephone Number: 513-684-2884
Facsimile Number: 513-684-6224

CLEVELAND AREA OFFICE
Cleveland Area Coordinator
Renaissance Building
1350 Euclid Avenue, Suite 500

OHIO STATE OFFICE
Ohio State Coordinator,
200 North High Street
Columbus, OH 43215-2499
Telephone Number: 614-469-5737
Facsimile Number: 614-469-2432

SPRINGFIELD AREA OFFICE
Springfield Area Coordinator
509 West Capitol Street, Suite

Springfield, IL 62704-1906
Telephone Number: 217-492-4085
Facsimile Number: 217-492-4971

WISCONSIN STATE OFFICE
Wisconsin State Coordinator,
Henry S. Reuss Federal Plaza

Cleveland, OH 44115-1815
Telephone Number: 216-522-4065
Facsimile Number: 216-522-2975

FLINT AREA OFFICE
Flint Area Coordinator
The Federal Building
605 North Saginaw, Suite 200
Nebraska, Flint, MI 48502-2043
Telephone Number: 810-766-5108
Facsimile Number: 810-766-5122

GRAND RAPIDS AREA OFFICE
Third Floor
Trade Center Bldg.
50 Louise St., NW
Grand Rapids, MI 49503-2648
Telephone Number: 616-456-2100
Facsimile Number: 616-456-2191

ILLINOIS STATE OFFICE
Secretary's Representative
Ralph H. Metcalfe Federal Building
77 West Jackson Boulevard
Chicago, IL 60604-3507
Telephone Number: 312-353-5680
Facsimile Number: 312-353-0121

INDIANA STATE OFFICE
Indiana State Coordinator
151 North Delaware Street
Indianapolis, IN 46204-2526
Telephone Number: 317-226-6303
Facsimile Number(12th Floor): 317-226-6317

MICHIGAN STATE OFFICE
Michigan State Coordinator
Patrick V. McNamara Federal Building
477 Michigan Avenue
Detroit, MI 48226-2592
Telephone Number: 313-226-7900
Facsimile Number: 313-226-4394

MINNESOTA STATE OFFICE
Minnesota State Coordinator
220 Second Street, South
Minneapolis, Minnesota 55401-2195
Telephone Number: 612-370-3000
Facsimile Number: 612-370-3220

310 West Wisconsin Avenue, Suite 1380
Milwaukee, WI 53203-2289
Telephone Number: 414-297-3214
Facsimile Number: 414-297-3947

GREAT PLAINS FIELD OFFICES
(Kansas, Missouri, Iowa,
St. Louis)

KANSAS/MISSOURI STATE OFFICE
Secretary's Representative,
Gateway Tower II
400 State Avenue
Kansas City, KS 66101-2406
Telephone Number: 913-551-5462
Facsimile Number: 913-551-5416

IOWA STATE OFFICE
Iowa State Coordinator,
Federal Building
210 Walnut Street, Room 239
Des Moines, IA 50309-2155
Telephone Number: 515-284-4512
Facsimile Number: 515-284-4743

NEBRASKA STATE OFFICE
Nebraska State Coordinator,
Executive Tower Centre
10909 Mill Valley Road
Omaha, NE 68154-3955
Telephone Number: 402-492-3100
Facsimile Number: 402-492-3150

ST. LOUIS AREA OFFICE
St. Louis Area Coordinator,
Robert A. Young Federal Building
1222 Spruce Street, Third Floor
St. Louis, MO 63103-2836
Telephone Number: 314-539-6583
Facsimile Number: 314-539-6575

ROCKY MOUNTAINS FIELD OFFICES
(Colorado, Wyoming, North Dakota,
Montana, Utah, South Dakota)
Sacramento,

PACIFIC/HAWAII FIELD OFFICES
(California, Fresno, Hawaii, Los
Angeles, Arizona, Reno,

San Diego, Santa Ana, Nevada,

Tucson)

COLORADO STATE OFFICE
Secretary's Representative
First Interstate Tower North
633 - 17th Street
Denver, CO 80202-3607
Telephone Number: 303-672-5440
Facsimile Number: 303-672-5061

WYOMING STATE OFFICE
Wyoming State Coordinator
Federal Office Building
100 East B Street, Room 4229
Post Office Box 120
Casper, WY 82602-1918
Telephone Number: 307-261-5252
Facsimile Number: 307-261-5251

NORTH DAKOTA STATE OFFICE
North Dakota State Coordinator
Federal Building
653 2nd Avenue, Room 366
500
Fargo, ND 58108-2483
Telephone Number: 701-239-5136
Facsimile Number: 701-783-5249

MONTANA STATE OFFICE
Montana State Coordinator
Federal Office Building
301 South Park, Room 340
Drawer 10095
Helena, MT 59628-0095
Telephone Number: 406-449-5205
Facsimile Number: 406-449-5207

UTAH STATE OFFICE
Utah State Coordinator
257 Tower Building
257 East - 200 South, Suite 550
Salt Lake City, UT 84111-2048
Telephone Number: 801-524-5241
Facsimile Number: 801-588-6701

SOUTH DAKOTA STATE OFFICE
South Dakota State Coordinator
2400 West 49th Street, Suite I-201
Sioux Falls, SD 57105-6558
Telephone Number: 605-330-4223
Facsimile Number: 605-330-4465

CALIFORNIA STATE OFFICE
Secretary's Representative,
Phillip Burton Federal Building
and U.S. Courthouse
450 Golden Gate Avenue
Post Office, Box 36003
San Francisco, CA 94102-3448
Telephone Number: 415-556-4752
Facsimile Number: 415-556-4176

FRESNO AREA OFFICE
Fresno Area Coordinator,
1630 East Shaw Avenue, Suite 138
Fresno, CA 93710-8193
Telephone Number: 209-487-5033
Facsimile Number: 209-487-5344

HAWAII STATE OFFICE
Hawaii State Coordinator,
Seven Waterfront Plaza
500 Ala Moana Boulevard, Suite

Honolulu, HI 96813-4918
Telephone Number: 808-522-8175
Facsimile Number: 808-522-8194

LOS ANGELES AREA OFFICE
Los Angeles Area Coordinator,
1615 West Olympic Boulevard
Los Angeles, California 90015-3801
Telephone Number: 213-251-7122
Facsimile Number: 213-251-7096

ARIZONA STATE OFFICE
Arizona State Coordinator,
Two Arizona Center
400 North 5th Street, Suite 1600
Phoenix, AZ 85004-2361
Telephone Number: 602-379-4434
Facsimile Number: 602-379-3985

RENO AREA OFFICE
Reno Area Coordinator,
1575 Delucchi Lane, Suite 114
Reno, NV 89502-6581
Telephone Number: 702-784-5356
Facsimile Number: 702-784-5066

SACRAMENTO AREA OFFICE
Sacramento Area Coordinator,
777-12th Street, Suite 200
Sacramento, CA 95814-1997
Telephone Number: 916-498-5220
Facsimile Number: 916-498-5262

SAN DIEGO AREA OFFICE
San Diego Area Coordinator
Mission City Corporate Center
2365 Northside Drive, Suite 300
San Diego, CA 92108-2712
Telephone Number: 619-557-5310
Facsimile Number: 619-557-6296

SANTA ANA AREA OFFICE
Santa Ana Area Coordinator
3 Hutton Centre Drive, Suite 500
Santa Ana, CA 92707-5764
Telephone Number: 714-957-3741
Facsimile Number: 714-957-1902

NEVADA STATE OFFICE
Nevada State Coordinator
Suite 700
Atrium Building
333 No. Ranano Drive
Las Vegas, NV 89106-3714
Telephone Number: 702-388-6500
Facsimile Number: 702-388-6736

TUCSON AREA OFFiCE
Tucson Area Coordinator
Security Pacific Bank Plaza
33 North Stone Avenue, Suite 700
Tucson, AZ 85701-1467
Telephone Number: 602-670-6237
Facsimile Number: 602-670-6207

NORTHWEST/ALASKA FIELD OFFICES
(Washington, Alaska, Idaho, Oregon, Spokane)

WASHINGTON STATE OFFICE
Secretary's Representative
Seattle Federal Office Building
909 1st Avenue, Suite 200
Seattle, WA 98104-1000
Telephone Number: 206-220-5101
Facsimile Number: 206-220-5133

ALASKA STATE OFFICE
Alaska State Coordinator
University Plaza Building
949 East 36th Avenue, Suite 401
Anchorage, AK 99508-4399
Telephone Number: 907-271-4170
Facsimile Number: 907-271-3667

IDAHO STATE OFFICE
Idaho State Coordinator
Plaza IV

SPOKANE AREA OFFICE
Spokane Area Coordinator,
Farm Credit Bank Building
Eight Floor East
West 601 First Avenue
Spokane, WA 99204-0317
Telephone Number: 509-353-2510
Facsimile Number: 509-353-2513

800 Park Boulevard, Suite 220
Boise, ID 83712-7743
Telephone Number: 208-334-1990
Facsimile Number: 208-334-9648

OREGON STATE OFFICE
Oregon State Coordinator
400 S.W. Sixth Avenue - Suite 700
Portland, OR 97204-1632
Telephone Number: 503-326-2561
Facsimile Number: 503-326-3097

Appendix C
THE PRIVACY ACT OF 1974
(As Amended, 1988)

5 U.S.C. § 552a

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, that this Act may be cited as the "Privacy Act of 1974."

SECTION 2

(a)

The Congress finds that --

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protect ions are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to --

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from such requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) 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 this Act.

SECTION 3

Title 5, United States Code, is amended by adding after section 552 the following new section:

552a. Records maintained on individuals

(a) DEFINITIONS

For purposes of this section --

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means 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;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(8) the term "matching program" --

(A) means any computerized comparison of --

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of --

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under' Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(B) but does not include --

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

(iv) matches of tax information --

(I) pursuant to section 6103(d) of the Internal Revenue Code of 1986;
(II) for purposes of tax administration as defined in section 6103 (b) (4) of such Code;
(III) for the purpose of intercepting a tax refund due an individual under authority granted by section 464 or 1137 of the Social Security Act; or
(IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and "Budget to contain verification, notice, and hearing requirements that are substan- tially similar to the procedures in section 1137 of the Social Security Act;

(v) matches --

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or
(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term "non-Federal agency" means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching

program,

(12) the term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the

Government of the United States (including survivor benefits)

(b) CONDITIONS OF DISCLOSURE

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a) (7) of this section and described under subsection (e) (4) (D) of this section;

(4) 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;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) 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;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal 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 which maintains the record specifying the particular portion

desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives. in the course of the performance of the duties of the General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(f) of title 31.

(c) ACCOUNTING OF CERTAIN DISCLOSURES

Each agency, with respect to each system of records under its control, shall --

(1) except for disclosures made under subsections (b) (1) or (b) (2) of this section, keep an accurate accounting of --

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection lb) of this section;

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b) (7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the

disclosure was made.

(d) ACCESS TO RECORDS

Each agency that maintains a system of records shall --

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and --

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either --

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual

to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g) (1) (A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) AGENCY REQUIREMENTS

Each agency that maintains a system of records shall --

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which' it uses to collect the information or on a separate form that can be retained by the individual --

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether the disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4) (D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include --

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records maintained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b) (2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure 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;

(11) at least 30 days prior to publication of information under paragraph (4) (D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) AGENCY RULES

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall--

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e) (4) of this section in a form available to the public at low cost.

(g) CIVIL REMEDIES

(1) Whenever any agency --

(A) makes a determination under subsection (d) (3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under (d) (1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the

individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2) (A) In any suit brought under the provisions of subsection (g) (1) (A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3) (A) In any suit brought under the provisions of subsection (g) (1) (B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine

whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably

incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g) (1) (C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of --

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where any agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

(h) RIGHTS OF LEGAL GUARDIANS

For the purpose of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i) CRIMINAL PENALTIES

(1) 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 this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

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

(j) GENERAL EXEMPTIONS

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c) (1), and (2), (e) (4) (A) through (F), (e) (6), (7), (9), (10), and (11), and (i) if the system of records is --

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional probation, pardon, or parole authorities, and which consists of --

(A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, parole and probation status;

(B) information compiled for the purpose of a criminal investigation; including reports of informants and investigations, and associated with an identifiable individual; or

(C) reports identifiable to an individual compiled at any stage of the process of enforcement or criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) SPECIFIC EXEMPTIONS

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c) (3), (d), (e) (1), (e) (4) (G), (H), and (I) and (f) of this section if the system of records is --

(1) subject to the provisions of section 552(b) (1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j) (2) of this section: provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protection services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;

or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(l) ARCHIVAL RECORDS

(1) Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred 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, prior to the effective date of this section,

shall, for the purposes of this section be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e) (4) (A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred 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, on or after the effective date of this section, shall be considered to be maintained by the National Archives and shall be exempt from the, requirements of this section except subsections (e) (4) (A) through (G) and (e) (9) of this section.

(m) GOVERNMENT CONTRACTORS

(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish

an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(J) of title 31 shall not be considered a contractor for purposes of this section.

(n) MAILING LISTS

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) MATCHING AGREEMENTS

(1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or

between the source agency and the recipient agency or non-non-Federal agency specifying --

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to --

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel, that any information provided by such

applicants, recipients, holders, and individuals may be subject to verification through matching programs;

(E) procedures for verifying information produced in such matching program as required by subsection (p);

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

(J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and

(K) that the Comptroller General may have access to all records of a recipient agency or non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2) (A) A copy of each agreement entered into pursuant to paragraph (1) shall --

(i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and

(ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A) (i)

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if --

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until--

(A) (i) the agency has independently verified the information; or

(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that --

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C) (i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no time period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to

the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including, where applicable, investigation and confirmation of --

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) SANCTIONS

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency of non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p) , or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless--

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) REPORT ON NEW SYSTEMS AND MATCHING PROGRAMS

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) 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 in order to permit an evaluation of the probable effect of such proposal on the privacy or other rights of individuals.

(s) BIENNIAL REPORT

The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report --

(1) describing the actions of the Director of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;

(2) describing the exercise of individual rights of access and amendment under this section during such years;

(3) identifying changes in or additions to systems of records;

(4) containing other such information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t) EFFECT OF OTHER LAWS

Relationship of the Privacy Act to the Freedom of Information Act.

(1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) DATA INTEGRITY BOARDS

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector

general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board --

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, and agency agreements, and assess the cost and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including-

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in the membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4) (A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5) (A) If a matching agreement is disapproved by a Data Integrity Board, any party to such an agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and

Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that--

(i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;

(ii) there is adequate evidence that the matching agreement will be cost-effective; and

(iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching

program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3) (D). Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and submission of a cost-benefit analysis and the reasons for granting the waiver.

(7) In the reports required by paragraphs (3) (D) and (6), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) OFFICE OF MANAGEMENT AND BUDGET RESPONSIBILITIES

The Director of the Office of Management and Budget shall-

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

SECTION 6 [Repealed]

SECTION 7

(a) (1) It shall be unlawful for any Federal, state, or local government
agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to-

(A) any disclosure which is required by Federal statute; or,

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

RULES OF CONSTRUCTION

Nothing in the amendments made by this Act shall be construed to authorize --

(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records maintained by other Federal agencies;

(2) the direct linking of computerized systems of record maintained by Federal agencies;

(3) the computer matching of records not otherwise authorized by law; or

(4) the disclosure of records for computer matching except to a Federal, State, or local agency.

EFFECTIVE DATES

(a) IN GENERAL. Except as provided in subsection (b) , the amendments made by this Act shall take effect 9 months after the date of enactment of this Act.

(b) EXCEPTIONS. The amendments reflected in subsections (f), (r), (v), and (s) shall take effect upon enactment.

Appendix D
APPEAL PROCEDURES

D-1 APPEAL FROM INITIAL DENIAL OF ACCESS TO RECORDS. The Privacy Appeals Officer will review any initial denial for access to records only if a written request for 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. If the appeal package fails to provide the required information the Privacy Appeals Officer will give the requester reasonable opportunity to amend the request and will advise that the time of receipt for processing purposes will be the time when the additional necessary information is received by the Privacy Appeals Officer.

C. If the request for appeal is misdirected, the Department official receiving it will promptly refer the request to the Privacy Appeals Officer, who is the General Counsel; the time of receipt of the request for processing purposes is the time the Privacy Appeals Officer receives it.

D. When all the necessary information is provided, the Privacy Appeals Officer will act on the appeal and issue a final determination in writing within 30 working days from the date on which the appeal is received. If the Privacy Appeals Officer determines that a fair and equitable review cannot be made within that period, then the period may be extended to 60 working days from receipt of the request for appeal. The individual must be advised in writing of the decision to extend the review period, the reason for the extension and the estimated date by which a final determination will be reached (within the 60 working day limitation)

1. If unusual circumstances exist (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; consultations with other agencies having a substantial interest in the determination are necessary), the 60-day review period may be further extended; however, only if

the individual is notified of this decision and the reason(s) for it in writing.

2. The Privacy Appeals Officer will not conduct hearings in connection with administrative review of an initial denial of access to a record.

E. The Privacy Appeals officer will render a decision in writing, which will constitute final action on the part of the Department on a request for access to a record. If the denial of the request is upheld, in whole or in part, the Privacy Appeals Officer will notify the requester of the right to judicial review under the provisions of the Privacy Act and the Departmental Regulations.

D-2 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.

A. The appeal package must contain:

1. A copy of the original request for correction or amendment.

2. A copy of the initial denial.

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

4. The individual's signature.

B. If the appeal package fails to provide the required information, the Privacy Appeals Officer will give the requester reasonable opportunity to amend the request and will advise him that the time of receipt of the appeal for processing purposes will be the time when the additional necessary information is received by the Privacy Appeals Officer.

C. If the request for appeal is misdirected, the Department official receiving it will promptly refer the request to the Privacy Appeals Officer; the time of receipt of the request for processing purposes is the time the Privacy Appeals Officer receives it.

D. The appeal package, received from the individual, and the record in question, to be supplied by the Privacy Act Officer who issued the initial denial, will normally comprise the entire record on appeal. However, the Privacy Appeals Officer may seek additional information to assure that the final determination is fair and equitable. In such instances the Privacy Appeals Officer will disclose this additional

information to the greatest extent possible to the individual and provide him with the opportunity to comment on the information disclosed.

E. When all the necessary information is provided, the Privacy Appeals Officer will act on the appeal and issue a final determination in writing within 30 working days from the date when all necessary information is received. If the Privacy Appeals Officer determines that he cannot make a fair and equitable review within that period, then the period may be extended to no more than 60 working days from receipt of the request for appeal. The individual must be advised in writing of the decision to extend the review period, the reason for the extension, and the estimated date by which a final determination will be reached (within the 60 working day limitation).

1. If unusual circumstances exist (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; consultations with other agencies having a substantial interest in the determination are necessary), the review period may be extended to 60 days; however, only if the individual is notified of this decision in writing.

2. The Privacy Appeals Officer will not conduct hearings in connection with administrative appeal of an initial denial to correct or amend a record.

3. The Privacy Appeals Officer will consider the following criteria in making a final determination on an appeal from a denial to correct or amend a 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 the 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.

4. The Privacy Appeals Officer may not uphold a denial of a request to correct or amend a record except under the following highly selective conditions:

a. The evidenced presented has failed to establish the propriety of the correction or amendment with regard to the criteria for considering a request to correct or amend a record.

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

c. 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.

d. The correction or amendment would violate a duly enacted statute or promulgated regulation.

e. The individual has unreasonably failed to comply with the procedural requirements for requesting a correction or amendment or for appealing a denial of a request to correct or amend a record.

F. If the appeal is granted, the Privacy Appeals Officer will inform both the individual and the Privacy Act Officer who issued the initial denial of the decision in writing. The notification will include the specific corrections or amendments to be made.

1. The Privacy Act Officer will 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 agency and an accounting made of the disclosure, the Privacy Act Officer will notify all such persons and agencies of the correction or amendment.

2. 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.

G. If the appeal is denied, the Privacy Appeals Officer will promptly notify the individual of the determination and state the reasons for denying the appeal. The Privacy Appeals Officer will also notify the individual of his rights as follows:

1. The individual may file a concise statement of reasons for disagreeing with the final determination.

   a. The statement should contain the date of the final determination and the individual's signature, and be filed with the Privacy Appeals Officer, who will

   acknowledge receipt of the statement, including the date on which it was received.

   b. The Privacy Appeals Officer and the Departmental Privacy Act Officer will jointly determine whether to accept or reject a statement of excessive length, typically greater than one page.

   c. Any such disagreement statement will be noted in the disputed record and a copy will be provided to persons or agencies to which the record was disclosed subsequent to the date of receipt of such statement, providing an accounting was made of the disclosure.

   d. The Department will append to any such disagreement statement a copy or summary of the final determination which will also be provided to persons or agencies to which the disagreement statement is disclosed.

   e. Although the copy or summary of the final determination is a part of the individual's record for purposes of disclosure, it will not be subject to correction or amendment by the individual.

2. The individual may obtain judicial review under the provisions of the Privacy Act and the Departmental Regulations.

Appendix E

RESPONSIBILITIES OF PRIVACY ACT SYSTEMS MANAGERS

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

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

A. Initiate action:

1. to provide advance notice to Congress and OMB of intent to establish or alter a Privacy Act system; and,

2. to publish notice in the Federal Register of intent to establish or alter a Privacy Act system.

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

B. Ensure that the published Privacy Act system notice covering the system is current and accurate, with particular emphasis on ensuring that routine use statements are correct and accurate.

C. Restrict release of records/use of personal information. Do not disclose any record unless disclosure of the record would be:

1. To those officers and employees of the Department who require the information to perform assigned duties.

2. Required by the Freedom of Information Act.

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

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

Freedom of Information Act).

1. Retain the record ("accounting") for five years or the life of Privacy Act record, whichever is longer.

2. Give the record ("accounting") to the subject of the record, upon request.

E. Establish appropriate safeguards (1) to ensure the security and confidentiality of records, and (2) to protect against any anticipated threats or hazards to their security or integrity (Appendix H contains guidelines for establishing safeguards for records subject to the Privacy Act.)

F. Maintain only information on an individual that is relevant and necessary to accompany a purpose of the agency required, as required by statute or Executive Order of the President.

G. Maintain records with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness to an individual in any determination about him.

H. Keep no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained. The First Amendment protects an individual's right of free assembly, freedom of religion, speech and press, and to petition the Government.

I. Make reasonable efforts to assure that records are accurate, complete, timely, and relevant before releasing information from a record.

J. If a record is disclosed containing information about which an individual has filed a statement of disagreement, the system

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

K. Inform any recipient of information from a Privacy Act record of any correction or notation of dispute made to the record after the information was released to the recipient.

L. Attempt to notify the subject of a record if information is released under compulsory legal process.

M. Collect information directly from the subject to the greatest extent practicable.

N. Give each individual asked to supply information a Privacy Act Statement. The statement should contain the following

information:

1. The authority authorizing the collection of the information.

2. Whether the disclosure of the information is mandatory or voluntary.

3. The principal purpose(s) for which the information is to be used.

4. The routine uses which may be made of the information.

5. The effects on the individual, if any, of not providing all or any part of the requested information.

O. Ensure that all employees who are involved in maintaining the system are aware of their responsibilities for safeguarding the records and maintaining them in accordance with Privacy Act requirements. All HUD Offices have been provided with access to Computer Based Training (CBT) allowing ADP security training to be available on the Local Area Network (LAN). Refer to Handbook 2400.24 REV-1 for additional guidance relating to ADP security training.

P. Apply Privacy Act requirements to any contractor associated with a system.

Q. Be sensitive to unique requirements concerning Social Security Number i.e., when individuals are requested to disclose their social security numbers, they must be informed whether that disclosure is mandatory or voluntary, by what statutory or other authority such is number is solicited, and what uses will be made of it.

R. Use the Systems Development Methodology (SDM) as a reference in the planning, preparation, execution, and administration of HUD's various system development activities and business areas. A copy of the document is available from the Office of Information Policies and Systems (IPS), Systems Engineering Group (SEG), Development Technology Division (DTD) Mainframe Technology Branch.

S. Be aware of the Criminal Penalties provided in the Act.

1. Any officer or employee who, knowing disclosure of material is prohibited, "--willfully disclosures the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000."

2. Any officer or employee of any agency who will fully maintains a system of records without meeting the notice requirements shall be guilty of a misdemeanor and fined

not more than $5,000.

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

Appendix F

COMPUTER MATCHING PROGRAMS TIMETABLE

Copies of agreements and reports/notices can be sent to congress simultaneously, allowing 40 days before initiation of match. Portrayed below are estimates of time frames for allowing the complete clearance and processing of computer matching documentation. We are assuming with these time frames that the program office has been working in advance with the Privacy Act Officer (PAO) matching agencies, etc.

FOR AGREEMENTS:

Program Office	Clearance/Signature	Allowance Time
Prepares and submits signed agreement to DIB	DIB approves/disapproves DIB chairman signs	2-3 weeks
Forwards Agreement to other matching agency	Other matching agency's official & DIB sign	4 weeks
Sends original (signed) agreement to Privacy Act Officer (PAO)	PAO immediately submits 2 copies to Congress	40 days (before initiation of match)
Total (processing & clearance)		90 days

FOR NOTICES/REPORTS

Program Office	Clearance/Signature	Allowance Time
Prepares and submits to PAO	1. PAO puts into clearance. (OGC, affected Program Offices, & IPS)	2 weeks
	2. PAO prepares letters to OMB and Congress and obtains A/S (Admin) signature (for sending copies of report/notice)	2 weeks
	3. PAO processes rpt/notice: a. Forwards notice for Federal Register publication. b. Sends signed A/S ltrs to OMB and Congress (with copies of report/notice).	40 days (before initiation of match)
Total (processing & clearance)		70 days

NOTE: If there is a current notice/report published which covers the specific computer matching programs, certain agreements may not require publication of a notice/report.

APPENDIX H
GUIDE TO THE PRIVACY ACT OF 1974 AND THE DEPARTMENTAL PRIVACY ACT REGULATIONS

H-1 YOUR RESPONSIBILITIES. Every individual has a right to privacy and under the Privacy Act the Department has certain responsibilities to ensure that right. 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, [5 USC 552a(b)], and in Departmental regulations, [24 CFR 16.11], which are discussed later under "Conditions of Disclosure."

B. Do not maintain unreported official files which would come under the Act, [5 USC 552a(e) (4), (e) (11) and (i) (2)].

C. Do not maintain records describing how any individual exercises the rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual, [5 USC 552a(e) (7)] The First Amendment protects an individual's right of free assembly, freedom of religion, speech and press, and to petition the Government.

H-2 DEPARTMENTAL RESPONSIBILITIES. The Department is responsible for assuring that the individual has access to his records, a right of consent or veto to any "non-routine use" transfer, and is given an accounting of all outside-the-agency transfers of his records. To safeguard those rights the Department must employ a set of procedures defined in the Act, [5 USC 552a], and Departmental Regulations, [24 CFR 16]:

A. Conditions of Disclosure. The Department will not disclose any record 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 [5 USC 552a(b)] and [24 CFR 16.11]:

1. Performance of duties by the officers and employees of the Department, [5 USC 552a(b)(1)] and 24 CFR 16.11(a) (5.(1))]

2. Required to be disclosed under the Freedom of Information Act, Title 5, Section 552 of the United States Code, [5 USC 552a(b) (2)] and 24 CFR 16.11(a) (5.(2))]

3. Routine use, as defined in Chapter 2, where the routine

use and the purpose of such use have been published in the Federal Register, [5 USC 552a(b) (3)] and [24 CFR 16.11(a) (5.(3))].

4. Planning or conducting a census or survey by the Bureau of the Census under the provisions of Title 13 of the United States Code, [5 USC 552a(b) (4)] and [24 CFR 16.11(a) (5.(4))].

5. Solely for statistical research or reporting by an individual or agency that has given advance written assurance of its statistical use and that the record will be transferred in a form that is not individually identifiable, [5 USC 552a(b) (5)] and [24 CFR 16.11(a) (5.(5))].

6. Continued preservation for its historical or other value by the National Archives of the United States, or to determine whether the record has such value by the General Services Administration, [5 USC 552a(b) (6)] and [24 CFR 16.11 (a) (5.(6))].

7. A civil or criminal law enforcement activity by another agency or government jurisdiction under control of the United States, if the activity is authorized by law and the head of the agency has made a written request to the Department specifying the portion of the record(s) desired and the law enforcement activity for which it is needed, [5 USC 552a(b)(7)] and [24 CFR 16.11(2) (5.(7))]. 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.

8. 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, [5 USC 552a(b) (8)] and [24 CFR 16.11(a) (5.(8))]

9. Required by Congress or any committee, joint committee or subcommittee with appropriate jurisdiction, [5 USC 552a(b)(9)] and [24 CFR 16.11(a) (5.(9))]. If a request from a member of Congress is made pursuant to a constituent's request, the Congressman's request must be handled as if it came directly from the subject himself.

10. Performance of duties by the General Accounting Office, [5 USC 552a(b) (10)] and [24 CFR 16.11(a) (5.(10))]

11. Required by a court order having appropriate jurisdiction, [5 USC 552a(b) (11)] and [24 CFR 16.11(a) (5.(11))]

12. Any purpose authorized by the individual in writing, including having an accompanying person present while the individual has access to his record(s), [24 CFR 16.11(a) (1)].

13. Any purpose authorized by prior written consent of the individual, [24 CFR 16.11(a) (2)].

14. Required by a parent or legal guardian acting for the subject individual, [24 CFR 16.11(a) (3)].

15. Required by the Act, but not explicitly covered by the provisions of the Act, [24 CFR 16.11(a) (4)], including:

    a. Dissemination of a corrected or amended record, or a notation of a disagreement between the subject and the Department of any portion of the subject's record, if the record has been disclosed and an accounting of the disclosure was made, [24 CFR 16.11 (b) (1)]. This correction, amendment or notation must be disseminated to each person or agency shown on the accounting record.

    b. Disclosure by the Department or a District Court of the United States when a civil action is brought against the agency by the individual, [24 CFR 16.11(b) (2)]

    c. Release to the Privacy Protection Study Commission, when requested by its Chairman, [24 CFR 16.11(b) (3)].

    d. Disclosure to the Office of Management and Budget in its role of overseeing and assisting in implementing the Act, [24 CFR 16.11(b) (4)].

B. Accounting for Disclosure. The Department will keep an account of the disclosures it makes of an individual's record, except in certain cases allowed for in the Act and the Regulations, [5 USC 552a(c)] and [24 CFR 16.11(c)] :

1. The Department will keep an accurate account of all disclosures it makes of an individual's record(s), except for those disclosures made to Departmental officers and employees in the performance of their duties or those required under the Freedom of Information Act, [5 USC 552a(c) (1)].

2. The Department will keep its accounting of a disclosure of a record(s) for five years after the disclosure is made or for the life of the record(s), whichever is longer, [5 USC 552a(c) (2)]

3. The Department will make its accounting of disclosure available to the individual concerned, at his request, except for disclosures made for a civil or law enforcement activity, [5 USC 552a(c) (3)].

4. The Department will inform any person or agency, to whom a disclosure was made, about any correction, amendment or notation of disagreement made by the Department at the request of the individual concerned, if an account was kept of the disclosure, [5 USC 552a(c) (4)].

C. Access to Records. The Department guarantees the individual access to and the right to a copy of his records, and the opportunity to correct and/or amend his own records, [5 USC 552a(d)] and [24 CFR 16.4 & 16.8].

1. The Department will allow an individual upon his request, and in accordance with the constraints below, to review the record(s) pertaining to him, to have a copy made of all or any portion of the record(s) and to have a person of his own choosing accompany him. However, such review will not be permitted if:

   a. the record is subject to an exemption under the Act and the HUD regulations,

   b. the record is compiled in reasonable anticipation of a civil action or proceeding, or

   c. the individual has unreasonably failed to comply with the procedural requirements of the regulations, [5 USC 552a(d) (1)] and [24 CFR 16.4(a) & 16.5(e)]:

      (1) Copies may be mailed at the request of the individual, subject to payment according to an established schedule of fees, or the Department may elect to provide a copy by mail at no cost to the individual, [24 CFR 16.5(b) (2) (iii)]

      (2) The Department will supply any information and assistance to make the record(s) intelligible at the time of access, [24 CFR 16.5(c)].

      (3) The Department reserves the right to limit access to copies and abstracts of original records, particularly when the records are on automated data media, such as tape or disk, when the records contain information on other individuals or when deletion of information is permissible under the Act, such as investigatory material, [24 CFR 16.5(d)].

(4) In no event will the Department allow the individual access to original records, except under the direct supervision of the Privacy Act Officer or his designee. It is a crime to conceal, mutilate, obliterate or destroy any record filed in a public office, or to attempt

to do any of these acts, [24 CFR 16.5(d)].

2. Access to his record may be denied to an individual if the record is subject to an exemption under the Act claimed by the Department or by another agency responsible for the systems of records, [5 USC 552a(j) & (k)], and the regulations, [24 CFR 16.14 & 16.15]; if the record has been compiled in reasonable anticipation of a civil action or proceeding; if the individual unreasonably has failed to comply with procedural requirements of the regulations, [24 CFR 16.4 through 24 CFR 16.6(a)].

3. The individual may request a review of the initial denial of access by providing the following information addressed to the Privacy Appeals Officer: copy of original request for access, if in writing; a copy of the written denial; and a statement of the reasons why the initial denial is believed to be in error. The appeal shall be signed by the individual, [24 CFR 16.7].

4. The Department will permit the individual the opportunity to correct or amend a record pertaining to him, [5 USC 552a(d) (2)] and [24 CFR 16.8]

   a. The request should include the following information; specific identification of the record; specific wording to be deleted, if any; specific wording to be inserted, if any, and the exact place it is to be inserted or added; the basis for the correction; and all supporting documents and materials which substantiate the request, [24 CFR 16.8(e)].

   b. Upon receipt of the request, the Department will either make the requested correction and/or amendment or inform the individual of its refusal to amend in accordance with the request, including the reason, procedures for a review of the refusal, and the name and business address of the reviewing official, [5 USC 552a(d) (2)] and [24 CFR 16.9(a)].

   c. If the decision, is to correct and/or amend the record, the Privacy Act Officer will arrange to transmit the arrange to transmit the changes to

those persons and agencies to which uncorrected record was disclosed, if an accounting of the disclosure was made under the provisions of the Act, [24 CFR 16.9(b)].

d. The Department will not gather evidence for the individual, but does reserve the right to verify evidence submitted by the individual, [24 CFR 16.9(d)].

5. The Department must permit the individual whose request for a, correction of amendment is denied to appeal that decision, [5 USC 552a(d) (3)] and [24 CFR 16.10(a)(d)].

a. The individual's appeal papers must contain: a copy of the original request for correction or amendment; a copy of the initial denial; and a statement of the reasons why the denial is believed to be in error, [24 CFR 16.10(e)].

b. If the appeal reverses the initial denial, the correction or amendment will be made, [24 CFR 16.10(f)-(h)].

c. If the appeal upholds the initial denial, the individual has the right to file a concise statement describing his reasons for disagreeing with the agency and the right for judicial review of the Privacy Appeals Officer's decision, [24 CFR 16.10(i) (1)-(4)], [5 USC 552a(d) (3)] and [24 CFR 16.10(i) (5)].

6. If a record is disclosed containing information about which an individual has filed a statement of disagreement, the Department will note the portions of the record under dispute, supply a copy of the statement of disagreement and, if appropriate, a copy of the Department's reason(s) for not making the requested changes, to the agencies and individuals found in the accounting record, [5 USC 552a(d) (4)] and [24 CFR 16.10(e)].

7. None of the above, under sub-paragraph C, shall allow an individual access to any information compiled in anticipation of a civil action or proceeding, [5 USC 552a(d) (5)].

D. Agency Requirements. The Department's operating procedures with respect to the Act include the following:

1. Maintain only that information on an individual that is relevant and necessary to accomplish its purpose, as

required by statute or by Executive Order of the President, [5 USC 552a(e) (1)].

2. Collect information, as practical, directly from an individual when that information may result in an adverse action concerning his rights, benefits and privileges under Federal programs, [5 USC 552a(e) (2)].

3. Inform each individual who is asked to supply information, on the form which he uses to collect the information or on a separate form that can be retained by the individual, [5 USC 552a(e) (3)]:

   a. The authority authorizing the collection of the information.

   b. Whether the disclosure of the information is mandatory or voluntary.

   c. The principal purpose(s) for which the information is to be used.

   d. The routine uses which may be made of the information.

   e. The effects on the individual, if any, of not providing all or any part of the requested information.

4. Publish a notice in the Federal Register, at least annually, on the existence and character of each system of records maintained by the Department, [5 USC 552a(e) (4)].

5. Maintain all records with such accuracy, relevance, timeliness and completeness as is necessary to assure fairness to an individual in any determination about him, [5 USC 552a(e) (5) and (6)].

6. No records will be maintained on how an individual

exercises his rights guaranteed by the First Amendment, unless expressly authorized by statute or by the individual himself or pertinent to and within the scope of an authorized law enforcement activity, [5 USC 552a(e)(7)].

7. Make reasonable efforts to inform an individual when a record pertaining to him is disclosed to any person under compulsory legal process, when such process becomes a matter of public record, [5 USC 552a(e) (8)].

8. Establish rules of conduct for persons involved in the design, development, operation or maintenance of any

record, and instruct those persons on the rules and requirements for such activities, [5 USC 552a(e) (9)].

9. Establish administrative, technical and physical safeguards to ensure security and confidentiality of records which could result in harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained, [5 USC 552a(e) (10)].

10. Publish a notice in the Federal Register on any new use or intended use of information maintained by the Department, [5 USC 552a(e) (11)].

E. Agency Rules. The Act requires that each agency establish a set of rules which determine the processes of inquiry, disclosure, correction or amendment, appeal and fees for copying documents. Accordingly, the Department has established such procedures to accomplish the following:

1. Inquiries. Either oral or in writing (in which case, the envelope and the letter should have entered "PRIVACY ACT INQUIRY"), should include--name, address and telephone number of the inquirer; if a parent or legal guardian, the name, address and telephone number of the individual to whom the record pertains; certified or authenticated copy of proof of parentage or guardianship; citizenship status of the individual; 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; signature of the inquirer, if in writing, [5 USC 552a(f)

(1)] and [24 CFR 16.3(a) and (b) (1) (i)-(ix)].

2. The person giving the information described immediately above should know that it is authorized by the Privacy Act, that such disclosure is voluntary with no penalty for failure to respond, that the principal purpose of the information is for processing the inquiry, that the routine uses which may be made of this information are internal to the Department or to those agencies and uses described in the prefatory statement to the Department's published notice of systems of records, and that the effect of not providing all or part of the information may delay the Department's processing of the inquiry, [24 CFR 16.3(b) (2)] and (3)].

3. Access request can be made by the individual concerned either in person or in writing, or if he is a minor, by his parents or legal guardian.

a. In person, the individual will be required to show satisfactory proof of his identity; this proof may be a document with his photograph, a document with

his signature or a signed statement asserting his identity and stipulating his understanding of the penalty under the Act for falsely seeking information on another individual, [5 USC 552a(f)(2)] and [24 CFR 16.4(a) and (d) (1)].

b. In writing, the person making the request should mark the letter and the envelope with "PRIVACY ACT Request FOR ACCESS TO RECORDS" and the letter should contain the same information as required for an inquiry as to the existence of a record. The letter should also contain a notarized certificate of identity. If the request for access follows an inquiry, this should be mentioned in the letter to facilitate processing, [24 CFR 16.4(d) (2)].

c. Parents of minors and legal guardians must, in addition to following the requirements for an oral written request for access, also furnish proof of parentage, such as a valid copy of the minor's birth certificate, or of guardianship, such as a

valid copy of the court's order, [24 CFR 16.4(d) (3)].

d. If the requirements for proof of identify are considered by the requester to be impeding his right to access to the record(s), the Department will consider alternate suggestions from the requester, [24 CFR 16.4(e)].

e. In no case will an individual have to state his reason for wishing access to a record, [24 CFR 16.4(f)].

4. Disclosure of requested information will be made to the individual provided that the system of records containing that information has not been exempted from the provisions of the Act, [5 USC 552a(f) (3)] and [24 CFR 16.5(b)].

a. The individual may have access to the record(s) in an office and at a time specified by the Privacy Act Officer; the record(s) may be transferred to a more convenient Federal facility, with the approval of the Privacy Act Officer; copies can be mailed to the individual at his request, subject to the payment of prescribed fees; or the Department may elect to provide a copy by mail at no cost to the individual, [24 CFR 16.5(b) (1) (i)-(iii) and (2) (i)-(iii)].

b. The individual may be accompanied by one or more persons of his choosing during access and disclosure [5 USC 552a(d) (2)] [24 CFR 16.5(b) (1)

(iv)] and [24 CFR 16.5(e)].

5. Denial of access to a record will be made by the Department if the record is subject to an exemption under the Act; compiled in reasonable anticipation of a civil action or proceeding; or if the individual unreasonably has failed to comply with procedural requirements, [24 CFR 16.6(a)]

   a. The individual may request a review of a denial for access within 30 working days by addressing a written request to the Privacy Appeals Officer marked "PRIVACY

   ACT REQUEST FOR REVIEW" on the envelope and in the letter, [24 CFR 16.7(a) and (b)].

   b. If the review upholds the denial in part or in whole, the Department will notify the individual of his right to judicial review, [24 CFR 16.7(h)].

6. Corrections or amendments to a record may be requested orally or in writing (in which case the envelope and the letter should be marked "PRIVACY ACT REQUEST FOR CORRECTION OR AMENDMENT")and should include specific identification of the record to be corrected or amended; specific wording to be deleted, if any; specific wording to be added, if any, and the exact location; and the basis for the request, including all substantiating documents and materials, [5 USC 552a(f) (4)] and [24 CFR 16.8(a) and (e) (1)-(4)] Correction or amendment of a record can be denied by the Privacy Act Officer only if, [24 CFR 16.9(e)] :

   a. The evidence presented fails to establish the need or propriety for the change, [24 CFR 16.9(e) (1)]

   b. The record was compiled in a pending or terminated judicial, quasi-judicial, legislative or quasi-legislative proceeding, of which the individual is or was a party or participant, [24 CFR 16.9(e) (2) and (3)].

   c. The correction or amendment would violate a duly enacted statue or regulation, [24 CFR 16.9(e) (4)].

   d. The request has unreasonably failed to comply with the procedures of the Department, [24 CFR 16.9(e) (5)].

7. Appeal of a denial for correction or amendment of a record may be made in writing up to 30 working days of the notification of denial, with both the letter and the envelope marked "PRIVACY ACT APPEAL," and should include: a copy of the original request for correction or amendment; a copy of the initial denial; a statement of

the reasons why

the denial should be reversed; the individual's signature, [5 USC 552a(f) (4)] and [24 CFR 16.10(a), (b) and (e)].

a. If the appeal is denied the individual will be informed of his right to file a concise (approximately one page) statement of disagreement with the final determination, which will be noted in the disputed record(s) and will be provided to any person or agency to whom the record is disclosed or to whom it has been already disclosed, if an accounting was made of such a disclosure, and of his right to judicial review of the final determination, [5 USC 552a(f) (4)] and [24 CFR 16.10(a), (b), (e) and (i) (1) - (5)].

8. General and Specific Exemptions. The Act provides for the exemption of certain classes of systems of records from the provisions of the Act with regard to inquiry, access, disclosure, appeal and judicial review, [5 USC 552a(j) and (k)] and [24 CFR 16.14 and 16.15].

a. The kinds of systems of records for which the Department may exercise an exemption are:

(1) investigatory material compiled for law enforcement purposes other than material compiled by a principally law enforcement agency;

(2) required by statute and used solely as statistical records;

(3) investigatory material compiled solely for the purpose of determining suitability, eligibility or qualifications for Federal employment and suitability for employment on Federal contracts or for access to classified information; and,

(4) compiled solely for the purposes of determining individual qualifications for appointment or promotion in the Federal service (testing or examination material) or in the armed services (recommendations), [5 USC 552a(j) (1)-(2) and (k) (11(7)].

b. The Department may not exempt any system of records from the following requirements:

(1) the constraints of the conditions of disclosure;

(2) from accounting for disclosures (except to employees of the Department in the performance of their duties or under the Freedom of Information Act);

(3) from retaining the accounting records for the life of the individual's record or five years after the disclosure is made, whichever is longer;

(4) from publishing in the Federal Register, at least once a year, a notice on the existence and character of the system of records;

(5) from assuring the accuracy, completeness, timeliness and relevancy of the record(s);

(6) from not describing how an individual exercises his rights guaranteed by the First Amendment;

(7) from establishing rules of conduct involving the design, development, operation or maintenance of the records;

(8) from establishing administrative, technical and physical safeguards to ensure the security and confidentiality of the records; or,

(9) from criminal penalties for willfully disclosing materials in any manner to any person or agency not entitled to receive them, [5 USC 552a(j) and (k)].

9. New Systems. The Department must provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records to permit an evaluation of the probable or potential effect of such proposals on the privacy of individuals or the disclosure of information in relating

to them, [5 USC 552a(o)].

a. Each employee who initiates a proposed new or altered system of records containing information on individuals is responsible for reporting this system of records directly to the Privacy Act Officer.

10. Miscellaneous Safeguards. The Act makes a number of

other provisions for safeguarding an individual's privacy and/or for identifying persons with regard to access and disclosure. A brief discussion of each follows:

a. The parent of a minor or the legal guardian of any individual declared incompetent by a court may act for the individual with respect to the Privacy Act, [5 USC 552a(h)].

b. Any record which is stored with the General Services Administration is still considered to be maintained by the Department and can be released only to the Department or its designated representative by the Administrator of the General Services Administration, [5 USC 552a(1) (1)].

(1) Any record sent to the National Archives of the United States for its use as a historical document is considered to be maintained by that Agency and the Department is relieved of Privacy Act responsibility, [5 USC 552a(1) (2) and (3)].

c. Any contractor, and any employee of the contractor, operating, on behalf of the Department, a system of records to accomplish a Departmental function is subject to the criminal penalties of the Act and is considered to be an employee of the Department for that purpose. The Department continues to be responsible for meeting the Act's requirements, [5 USC 552a(m)].

d. An individual's name and address may not be sold or rented by the Department unless specifically authorized

by law, but such information cannot be withheld if otherwise permitted to be made public, [5 USC 552a (n)].

e. The Department cannot use exemptions under the Freedom of Information Act to withhold from an individual any record which is otherwise accessible to the individual under the provisions of the Privacy Act, [5 USC 552a (t)].

11. Civil Actions and Criminal Penalties. The Privacy Act makes provision for an individual to bring a suit against the Department if the Department has failed in its duties with regard to inquiry, access, correction and amendment, or if an officer or employee of the Department will fully discloses material, does not meet privacy requirements for maintaining a record, or will fully requests or obtains information under false pretense, [5 USC 552a(g) and (i)] and [24 CFR 16.13]:

a. Civil actions may be brought against the Department in the District Courts of the United States if it has failed in its duties under the Act as follows:

(1) The Department refuses to review its denial to correct or amend an individual's record(s), or, if a review upholds the initial denial, refuses to allow the individual to file a statement of disagreement with the denial, and/or does not notify the individual of his rights for judicial review, following the upholding of a denial, [5 USC 552a (g) (1) (A) and (d) (3)].

(2) The Department refuses to allow the individual to have a person or persons accompany him while his records are being accessed and disclosed, [5 USC 552a (g) (1) (B) and (d) (1)].

(3) The Department fails to maintain any of an individual's records with such accuracy, relevancy, timeliness and completeness, or fails to comply with any provisions of the Act or Departmental Privacy Act regulations as

to have an adverse effect on the individual, [5 USC 552a(g) (1) (C) and (D)].

(4) In any suit brought against the Department because it refuses to review a denial to correct or amend an individual's record(s) or because it refuses to allow a person to accompany the individual during access and disclosure of his record(s), the court may order the Department to amend the individual's record(s) according to his request, to deliver any record(s) to the individual that was improperly withheld from him, and to pay reasonable attorney fees and other litigation costs, [5 USC 552a(g) (2) and (3)].

(5) In any suit brought against the Department because it intentionally or will fully maintained records or failed to comply with the Act or Departmental Privacy Act regulations in such a way as to have an adverse effect on the individual, the court may order the United States to pay damages of not less than $1,000 and the costs of the action, plus reasonable attorney fees, [5 USC 552a(g) (4)].

(6) A civil action can be brought in a District

Court of the United States within two (2) years of the date on which the course of the action occurred, except where the Department has materially and will fully misrepresented any information under the Act to be disclosed to an individual, in which case, a civil action can be brought into court within two (2) years after the misrepresentation is discovered, [5 USC 552a(g) (5)].

b. Criminal penalties are provided under the Act, up to $5,000, for any Department Officer or employee or any other person found guilty of a misdemeanor for one of the following activities:

(1) Any Department Officer or employee who has possession of or access to systems of records which are under the Act and knowingly and willfully discloses these records in any manner to any person or agency not entitled to receive them is guilty of a misdemeanor, [5 USC 552a(i) (1)].

(2) Any Department Officer or employee who will fully maintains a system of records and who does not publish an annual notice in the Federal Register of the existence and character of the system shall be guilty of a misdemeanor, [5 USC 552a(i) (2)].

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual under false pretenses shall be guilty of a misdemeanor, [5 USC 552a(i) (3)] and [24 CFR 16.13(a)]; and may also be subject to prosecution under other criminal statutes, [24 CFR 16.13(b)].

c. FEES. The fees to be charged an individual under the provisions of the Privacy Act and the Departmental Regulations are for copying records at his/her request: Manual record files should be the source for copying purposes unless a computer printout of the record is both readily available and readable (plain English). The following provisions affect the assessment of such fees, [5 USC 552a(f) (5)]:

(1) No fees will be charged or collected for the following:

(a) Search for the records.

(b) Review of the records.

(c) Copying at the initiative of the Privacy Act Officer without a request from the individual.

(d) Transportation of records and personnel.

(e) First class postage.

(f) One copy of each record corrected or amended pursuant to the individual's request as evidence of the correction or amendment.

(g) A single copy of a personnel record covered by the Office of Personnel Management's Government-wide published notice of systems of records. However, in cases where such records are voluminous the Department may, at its discretion, charge a fee when the cost would exceed five dollars ($5.00).

(2) Copying fees will be charged as prescribed below:

(a) Each copy of each page, up to 8 1/2" x 14" made by photocopy or similar process - $0.15.

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

(c) Each duplicated microfiche $1.00.

(d) Each duplicated roll of 16 mm microfilm $2.00 roll/cartridge.

(e) Each paper printout from microfilm/microfiche $0.15 per image/page.

(f) Prepayment can be made in cash, but preferably by check or money order payable to "Treasurer of the United States." In some cases the Privacy Act Officer may deem it appropriate to require payment in the form of a certified check. The payment should be paid or sent to the office stated in the

billing notice or, if none, to the

Privacy Act Officer processing the request.

(g) A copying fee of $1.00 or less shall be waived by the Privacy Act Officer, but the copying fees individually 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 disproportionately exceeds the amount of the fee.

(h) Special and additional services provided at the request of the individual, such as certification or authentication, postal insurance and special mailing arrangement costs will be charged to the individual in accordance with other published regulations of the Department.

U.S. Department of Housing and Urban Development

Appendix I

Special Attention of: Transmittal for Privacy Act Systems of Records

Privacy Act Officers
General Counsels
Regional Counsels
Chief Attorneys

Issued: January 1993

This transmits the Department's inventory of Privacy Act Systems of Records as published in the Federal Register, Privacy Act Issuances 1991 Compilation. One amendment (Attachment 1) and three new systems of records (Attachments 2 to 4) to the inventory, published in the Federal Register during calendar year 1992, are included as attachments.

An updated inventory will be provided biennially to Privacy Act Officers, General Counsels, Regional Counsels, and Chief Attorneys.

AII: Distribution: R-3-1 (RC), R-6, R-7, R-8.