

U.S. Department of Housing and Urban Development

**Inspector General
Office of Audit (OA)**

**AutoAudit
Privacy Impact Assessment**

February 2007

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **AutoAudit**. This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

- The document is accepted.**
 The document is accepted pending the changes noted.
 The document is not accepted.

Based on our authority and judgment, the data captured in this document is current and accurate.

/s/ Marcieta Thompson

SYSTEM MANAGER

Marcieta Thompson
OCIO, HUD OIG

3/8/07

Date

/s/ Karen Cookson

PROGRAM AREA MANAGER

Karen Cookson
Office of Audit

3/5/07

Date

DEPARTMENTAL PRIVACY ADVOCATE

Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

Date

/s/ Jeanette Smith

DEPARTMENTAL PRIVACY ACT OFFICER

Office of the Chief Information Officer
U. S. Department of Housing and Urban Development
Jeanette Smith

3/21/07

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT	7
Question 1: Provide a brief description of what personal information is collected.....	7
Question 2: Type of electronic system or information collection.....	9
Question 3: Why is the personally identifiable information being collected? How will it be used?	10
Question 4: Will you share the information with others?	12
Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?	12
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	12
Question 7: If privacy information is involved, by what data elements can it be retrieved?...	13
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	14

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
AUTOAUDIT**

**(for IT Systems: OMB Unique Identifier : *N/A*
and PCAS #: *N/A***

February 9, 2007

NOTE: See Section 2 for PIA answers and Section 3 for Privacy Advocate's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See <http://www.usdoj.gov/foia/privstat.htm>; see also HUD Handbook 1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See <http://www.usdoj.gov/foia/privstat.htm>);
- Freedom of Information Act of 1966, as amended (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also HUD's Freedom of Information Act Handbook (HUD Handbook 1327.1 at www.hudclips.org);
- E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- Federal Information Security Management Act of 2002 (which superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security

regulations at Title 44 U.S. Code chapter 35 subchapter II (<http://uscode.house.gov/search/criteria.php>); and

- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).

2. Existing Systems: Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA): Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The Privacy Act of 1974, as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Advocate in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

Program Area: Office of Audit

Program Area Manager: Karen Cookson 202.708.0614 ext 8115 kcookson@hudoig.gov

IT Project Leader: Marcieta Thompson 202.314.5471 mthompson@hudoig.gov

For IT Systems:

- **Name of system:** AutoAudit
- **PCAS #:** N/A **OMB Unique Project Identifier #:** N/A.
- **System Code:** N/A

For Information Collection Requests: N/A. Not a ICR AutoAudit is an existing system.

- **Name of Information Collection Request:** N/A
- **OMB Control #:** N/A

Question 1: Provide a brief description of what personal information is collected.

Background

The U. S. Department of Housing and Urban Development (HUD) Inspector General is one of the original 12 Inspectors General authorized under the Inspector General Act of 1978. The Office of Inspector General (OIG) is an independent and objective organization responsible for audits and investigations relating to program and operations of the Department.

The Office of Audit is an organizational unit within HUD OIG, which is responsible for the development and implementation of the Department's audit activities. This includes:

- A. Conducting and supervising independent and objective audits of agency programs and operations. This includes the authority to determine what audits to perform and to access all information necessary to complete the audits.
- B. Promoting economy, effectiveness, and efficiency within the agency.
- C. Preventing and detecting fraud, waste, and abuse in agency programs and operations.
- D. Reviewing and making recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- E. Keeping the agency head and the Congress fully and currently informed of problems in agency programs and operations.

The Office of Audit is led by the Assistant Inspector General for Audit (AIGA). The Office of Audit has a Headquarters Office organized into three divisions in Washington D.C., eight

Regional Offices, with Field Offices located within Regions, and an office for Hurricane Recovery. The Office of Audit employs approximately 300 staff.

AutoAudit for Lotus Notes

The Office of Audit (OA) uses a customized version of Paisley Consulting’s AutoAudit for Lotus Notes application for managing its audit operations in a “paperless” work environment. The AutoAudit application allows users to create and store all of their audit documentation, such as audit programs, workpapers, findings, memos, and audit reports in a Lotus Notes database where they can be easily retrieved for future use. It is important to note that AutoAudit is not a database used for retrieving privacy information.

Currently, there are about 300 AutoAudit users.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Social Security Number (SSN) .
<input checked="" type="checkbox"/>	Other identification number (specify type):
<input checked="" type="checkbox"/>	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
<input checked="" type="checkbox"/>	Personal e-mail address
	Fingerprint/ other “biometric”
	Other (specify): Relatives and Friends Names
	None
	Comment:

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
<input checked="" type="checkbox"/>	Gender/ sex
<input checked="" type="checkbox"/>	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
<input checked="" type="checkbox"/>	Employment history:
<input checked="" type="checkbox"/>	Education level
	Medical history/ information
	Disability
	Criminal record
	Other (specify):
	None

	Comment:
--	----------

Question 2: Type of electronic system or information collection.

Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)? **NO**

If yes, fill out subsections a, b, and c.

	Yes	Yes	No
	a. Does the system require authentication?	<input type="checkbox"/>	<input type="checkbox"/>
	b. Is the system browser-based?	<input type="checkbox"/>	<input type="checkbox"/>
	c. Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input type="checkbox"/>
X	No		
	Comment		

B. If an existing electronic system: YES. Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (if not applicable, mark N/A):

n/a	Conversion: When paper-based records that contain personal information are converted to an electronic system
n/a	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
n/a	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
n/a	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
n/a	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
n/a	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
n/a	New Inter-agency Uses: When agencies work together (such as the federal E-Gov

	initiatives), the lead agency should prepare the PIA
n/a	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
n/a	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

- C. If an Information Collection Request (ICR): **N/A**. Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.

	Yes, this is a new ICR and the data will be automated
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	Comment:

Question 3: Why is the personally identifiable information being collected? How will it be used?

Personally identifiable information collected in the course of conducting an audit is used to obtain and to afford a reasonable basis for the auditor’s opinions and conclusions to meet the required audit objective, i.e., to determine program eligibility. Personally identifiable information is collected on a case-by-case basis, as needed, to meet the required audit objective.

Auditors may collect personally identifiable information during the course of collecting audit evidence. Auditors’ findings and conclusions must be supported by sufficient, competent, and relevant evidence. Audit evidence may be categorized as physical, testimonial, documentary, or analytical. The auditors obtain physical evidence by direct inspection or observation of activities of people, property, or events, such as memoranda summarizing the matters inspected or observed photographs, charts, or actual graphs. The auditors obtain testimonial evidence through statements received in response to inquiries or through interviews. The auditors obtain documentary evidence, including letters, contracts, accounting records, invoices, cancelled checks, electronic documents such as electronic email, etc. The auditors obtain analytical evidence through computations, comparisons, separation of information into components, and rational arguments.

Personally identifiable information may also be collected by ad hoc queries of HUD’s automated systems such as the Real Estate Management System (REMS), the PIH Information Center (PIC), the Single Family Data Warehouse, the Tenant Rental Assistance Certification System (TRACS), etc. In addition, personally identifiable information may be collected by ad hoc queries of commercial sources such as ChoicePoint and LexisNexus.

Mark any that apply:

Homeownership:

<input checked="" type="checkbox"/>	Credit checks (eligibility for loans)
<input checked="" type="checkbox"/>	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
<input checked="" type="checkbox"/>	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
<input checked="" type="checkbox"/>	Loan default tracking
<input checked="" type="checkbox"/>	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

<input checked="" type="checkbox"/>	Eligibility for rental assistance or other HUD program benefits
<input checked="" type="checkbox"/>	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
<input checked="" type="checkbox"/>	Property inspections
	Other (specify): Fraud
	Comment:

Grants:

<input checked="" type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input checked="" type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

<input checked="" type="checkbox"/>	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

<input checked="" type="checkbox"/>	Employee payroll or personnel records
<input checked="" type="checkbox"/>	Payment for employee travel expenses
<input checked="" type="checkbox"/>	Payment for services or products (to contractors) – if any personal information on the payee is included
<input checked="" type="checkbox"/>	Computer security files – with personal information in the database, collected in order to grant user IDs
	Other (specify):
	Comment:

Other lines of business (specify uses):

Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
X	Others? (specify): HUD officials, as needed for programmatic purposes. In addition, the information may be shared with the AUSA if there is a pending case.
	Comment:

Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
X	No, they can’t “opt-out” – all personal information is required
	Comment:

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): Anonymous, Confidential Compliance

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password – YES
X	When an employee leaves: <ul style="list-style-type: none"> How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? 1 week. MAC Delete Request How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): Lotus Notes AdminP Process. Searches for users name and searches ACL for user and removes the user’s access.
X	Are access rights selectively granted, depending on duties and need-to-know?

	<p>Yes. Access is granted according to user role, Role Based Access Control (RBAC).</p> <p>If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> • Approximately 300 users • Full access rights to all data in the system: 3 personnel • Limited/restricted access rights to only selected data: 297
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve):</p> <p>Yes. Nightly incremental backup and weekly full backup. Stored in locked file cabinet in server room.</p>
	<p>If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? N/A</p> <p>Explain the existing privacy protections, or your plans to improve: N/A</p>
X	<p>Other methods of protecting privacy (specify):</p> <p>HUD OIG OCIO whole disk encryption initiative is underway using the SecureDoc, WinMagic's whole disk encryption product</p>
X	<p>Comment:</p> <p>AutoAudit is set up to limit the accessibility of the work papers to only the staff that need to have access. This can be limited even further, for example if the work involves Grand Jury testimony (6e).</p>

Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?

N/A. AutoAudit is not a database retrieval system for which privacy information is retrieved.

Mark any that apply

	Name:
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
X	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

Response to Question 6 indicates that the privacy of the information is protected. There is restricted access to the information granted according to user role, depending on duties and need-to-know. Also, AutoAudit is set up to limit the accessibility of the work papers to only the staff that need to access the information to perform their official duties. Additional protection will be provided through the whole disk encryption initiative presently underway.