

U.S. Department of Housing and Urban Development

Office of Fair Housing and Equal Opportunity

Title Eight Automated Paperless Office Tracking System (TEAPOTS)

Privacy Impact Assessment

09/05/2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **the Title Eight Automated Paperless Office Tracking System (TEAPOTS)**. 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/ NINA ATEN

PROGRAM AREA MANAGER

Nina Aten, Director, Office of Information Services
and Communications (FHEO)

9/5/2008

Date

/S/ KEVIN GILBERT

SYSTEM MANAGER

Kevin Gilbert, TEAPOTS Project Manager (FHEO)

9/5/2008

Date

DEPARTMENTAL PRIVACY ADVOCATE

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

Date

/S/ Donna Robinson-Staton

DEPARTMENTAL PRIVACY ACT OFFICER

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

09/09/08

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?	11
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?.....	13
Question 7: If privacy information is involved, by what data elements can it be retrieved?...	14
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	14

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
“TITLE EIGHT AUTOMATED PAPERLESS OFFICE TRACKING SYSTEM”
(TEAPOTS)”**

**OMB Unique Identifier: 02500010502000000301091
PCAS #308160**

09/05/2008

NOTE: See Section 2 for PIA answers and Section 3 for Privacy Act Officer’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) (<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) (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](http://www.usdoj.gov/foia/privstat.htm), 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 Act Officer 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 Act Officer 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 Federal Housing and Equal Opportunity

Subject matter expert in the program area: Kevin Gilbert, Management Information Specialist, Technology Support Branch, Federal Housing and Equal Opportunity, (202) 708-0875 Ext. 6931

Program Area Manager: Nina Aten, Director, Office of Information Services and Communication, Federal Housing and Equal Opportunity, (202) 708-0875

IT Project Leader: John Horn, Computer Specialist, Office of Systems Integration and Efficiency, Office of the Chief Information Officer, (202) 708-5495 Ext. 7434

For IT Systems:

- **Name of system:** Title Eight Automated Paperless Office Tracking System
- **PCAS #:** 00308160
- **OMB Unique Project Identifier #:** 02500010502000000301091
- **System Code:** E08A

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

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

TEAPOTS is an automated case management system that processes housing discrimination inquiries and complaints. It is used to develop, manage, track and report on inquiries and complaints filed under Title VIII of the Civil rights Act of 1968, as amended by the Fair Housing Act of 1989, as well other enforcement laws and processes. Housing discrimination complaints are brought to HUD by individuals and organizations and many of these complaints are investigated by investigators within FHEO or within a state or local agency that has partnered with HUD to do the investigations and to follow through with any legal processing necessary.

During the course of the investigation, the contact information of all complainants, respondents, witnesses, representatives and contacts will be recorded in TEAPOTS. Often the parties in a discrimination case are difficult to contact because they are moving, disabled, homeless, etc. Due to this problem, complainants are asked to submit contact information of a friend or relative as a backup.

There are no fields in TEAPOTS to collect race/ethnicity data of the parties, but the complainant may file a case based on a Basis (protected class as defined by law) of race/ethnicity for filing the case. All parties may be asked their race/ethnicity if it were relevant to the case, but this would show up in the narrative of an interview or the summary of a document. Gender/sex, spouse's name, number of children and marital status may also be included in a narrative text

field as it may be relevant to cases of sexual discrimination or discrimination against families with children and generally all parties affected by a discriminatory act are identified as complainants or aggrieved parties and this usually includes a spouse and children if they are housed together. Additionally the birthdates of minor children may be recorded to identify them as minors, which may be relevant to certain investigations.

Interviews will be conducted with the parties involved in the case and that data will be recorded in TEAPOTS. Often during interviews, additional personal information will be requested by the interviewer or it will be offered by the interviewee. This might include a medical or criminal history. Medical information may be relevant to a disabled person’s complaint.

Documents will be reviewed during the investigation and summaries of these documents will be recorded in TEAPOTS. Often the tenant files of tenants completely uninvolved in the complaint will be reviewed to determine how others may have been treated similarly or differently from the complainant. Contact information, tenant histories, credit histories, income, rent, etc. may be summarized in TEAPOTS if it is relevant to the case.

******TEAPOTS was re-platformed from a NetDynamics/SQL environment to a J2EE/Oracle environment. Production implementation took place August 2008. As part of the new release FHEO removed all the SSNs and SSN data entry fields from the TEAPOTS database. SSNs are no longer collected by this system.**

Currently TEAPOTS does not collect email addresses, but these fields will be added in a future upgrade to the system as an additional contact option.

The name of the investigator or conciliator is included in each case including in each interview and conciliation notation.

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

Personal/ Sensitive Information:

X	Race/ ethnicity
X	Gender/ sex
X	Marital status
X	Spouse name
X	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history:
	Education level
X	Medical history/ information
X	Disability
X	Criminal record
	Other (specify):
	None
X	Comment: There are no fields in TEAPOTS that specify personal/sensitive information be entered, but much of this information will be collected and recorded in interviews or document summaries only if it is relevant to the particular case. Only in cases involving disability discrimination would disability and medical history information be recorded. In cases where someone claims they have been treated differently due to their race it may be necessary to look at all the criteria the respondents had, which might have included their income, credit history, and criminal record.

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)? **If yes, fill out subsections a, b, and c.**

		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		

A. If an existing electronic system: 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):

X	Conversion: When paper-based records that contain personal information are converted to an electronic system
	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally

N/A	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) CLARIFICATION: New HUD certified business partner Fair Housing Assistance Program (FHAP) agencies are given access to collect and process fair housing cases under a cooperative agreement with HUD (as required by law).
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): 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
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
N/A	Comment: THIS IS NOT AN ICR

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

Mark any that apply:

Homeownership:

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

Rental Housing Assistance:

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

Grants:

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

Fair Housing:

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

Internal operations:

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

<input checked="" type="checkbox"/>	Federal agencies?
<input checked="" type="checkbox"/>	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
<input checked="" type="checkbox"/>	Local and national organizations? CLARIFICATION: HUD certified FHAP Agencies only
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
	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)?

<input checked="" type="checkbox"/>	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
	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):

Generally a person may opt-out, but if a complainant does not provide the basic facts necessary to investigate their complaint; their complaint will be closed. If the investigator is unable to contact the complainant after trying all of the possibilities provided by the complainant then the complaint will be closed. If witnesses decline to provide information that is okay though it may affect the outcome of the investigation. If the respondents decline to provide information they can be legally compelled to comply by a court of law.

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
X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <p>TEAPOTS has an Access Security Policy. It is posted on the TEAPOTS Homepage and was distributed to TEAPOTS HQ, Regional, Field, OGC and FHAP System Administrators and Manager. The policy reads as follows: FHEO HQ, Region, Field, OGC and FHAP personnel in charge of TEAPOTS Staff Maintenance; upon learning of an employee that should no longer have access to TEAPOTS, for any reason, must suspend that employee's TEAPOTS ID immediately. If your office has nobody in charge of TEAPOTS Staff Maintenance, you should contact your Regional TEAPOTS System Administrator immediately and request the employee's TEAPOTS access be suspended. Suspension shall be completed no later than 1 day after learning of the need to do so.</p>
X	<p>Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> • Full access rights to all data in the system: 1,235 • Limited/restricted access rights to only selected data: 1,510
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>Though TEAPOTS is planned to be part of a paperless system, it is currently used to store information that is also contained in a hard-copy case file. Certain hard copy forms submitted by FHAP agencies, as well as incoming correspondence from claimants, received by FHEO staff contain personal identifiable information (PII), including Social Security Numbers. These documents are photocopied for the purpose of redaction, and the original document is stored in a locked filing cabinet. The photocopy is then redacted to black out the Social Security Number. The redacted photocopy is then photocopied. The first redacted photocopy is then shredded. The second photocopy is used when information is taken out of the office for the investigative purposed or when staff telework from an alternate location. The plan for TEAPOTS is to add the ability to scan documents and remove the need for the paper-based file. Disks and tapes are secured.</p>
X	<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? Explain the existing privacy protections, or your plans to improve:</p>

	Data on closed cases is periodically provided to the National Archive and Records Administration (NARA), along with guidance indicating that the files include personal identifiable information and are NOT releasable based on the Privacy Act (5 U.S.C. 552a), and HUD's FHEO FOIA exemptions, (5 U.S.C. 552 (b) (5) and (6), and NARA is responsible for following those restrictions.
	Other methods of protecting privacy (specify):
	Comment:

Question 7: If privacy information is involved, by what data elements can it be retrieved?

Mark any that apply:

<input checked="" type="checkbox"/>	Name:
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Other (specify):
	None
<input checked="" type="checkbox"/>	Comment: Users are only able to retrieve information by the person's name. As mentioned above, spouses are often also listed as complainants.

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

TEAPOTS is a concern to privacy due to the personal and sensitive data collected by the system. However, we have determined that adequate administrative controls are in place for protecting such data. Please refer to question number 6, which clearly states the types of administrative controls in place.