Department of Housing and Urban Development

Public and Indian Housing Information Technology

Information Security Program

Tenant Assessment Sub-System

Privacy Impact Assessment

December 14, 2005

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the Tenant Assessment Sub-System (TASS). This document has been completed in accordance with the requirements set forth by Federal Information Security Management Act of 2002 (FISMA), Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Public and Indian Housing (PIH) Information Technology (IT) Office.

MANAGEMENT ENDORSEMENT

Please check the appropriate statement.

__X__ 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/ Eric M. Stout — **Dec. 14, 2005**
Departmental Privacy Advocate — **Date**

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

/s/ Jeanette Smith — **Dec. 14, 2005**
Departmental Privacy Act Officer — **Date**

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

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT ..... **i**

TABLE OF CONTENTS ..... **ii**

SECTION 1. BACKGROUND **1**

Importance of Privacy Protection – Legislative Mandates 1
What is the PIA Process? 2
Who Completes the PIA? 2
When is a PIA Required? 2
What are the Privacy Act Requirements? 3
Why is the PIA Summary Made Publicly Available? 3

SECTION 2. COMPLETING A PRIVACY IMPACT ASSESSMENT **4**

Question 1: Provide a brief description of what personal information is collected 4
Question 2: Type of electronic system or information collection 6
Question 3: Why is the personally identifiable information being collected? How will it be used? 7
Question 4: Will you share the information with others? 8
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)? 8
Question 6: How will the privacy of the information be protected/secured? What are the administrative and technical controls? 9
Question 7: If privacy information is involved, by what data elements can it be retrieved? 9

SECTION 3. DETERMINATION BY HUD PRIVACY ADVOCATE **10**

APPROVED/ FINAL

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

Tenant Assessment Sub-System (TASS)
(For Information Collections: OMB Control #: N/A)
(For IT Systems: OMB Unique Identifier: N/A)
PCAS # REAC - 307790
December 2005

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, the beneficiaries of HUD programs and business partners, and on its own employees. These individuals have a right to expect that HUD will collect, maintain, use, and disseminate personally identifiable information (PII) 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 Handbook1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988, which amends the Privacy Act of 1974, 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 public information that is maintained by Federal agencies, 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 PIAs on their 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 supersedes 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
- Office of Management and Budget (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 PII will be restricted to those staff who need the data to carry out their duties. Such staff will be held accountable for ensuring privacy and confidentiality of the data.

What is the PIA Process?

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

The PIA:

- Identifies the type of PII 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
- Defines the administrative controls which ensure that only necessary and relevant information to HUD's mission is included.

Who Completes the PIA?

The program area system owner and the information technology (IT) project leader work together to complete the PIA. The system owner describes what personal data types are collected, how the data are 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 to PII.

When is a PIA Required?

1. **New Systems.** According to OMB requirements, any new system, including major and non-major systems, containing personal information on members of the public requires a PIA.
2. **Existing Systems.** Where there are significant modifications involving personal information on members of the public, or where significant changes have 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?

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, by some other identifying number or symbol, or by other particular identifiers assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems and for information collection requests that are automated. Therefore, a relationship exists between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notice requirement (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 (OCIO).

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 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

Program Area: Office of Public and Indian Housing (PIH) – Information Technology (IT)
Subject Matter Expert in the Program Area: Elking Tarver

Program Area Manager: David Sandler

IT Project Leader: David Sandler

For IT Systems:

- **Name of system:** Tenant Assessment Sub-System (TASS)
- **PCAS #:** REAC – 307790
- **OMB Unique Project Identifier #:** 025-00-01-01-01-1010-00

For Information Collection Requests:

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

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

HUD developed and implemented an automated system called the Tenant Assessment Sub-System (TASS) to aid program administrators during the re-certification of tenants for participation in the rental assistance programs. HUD's Office of Public and Indian Housing (PIH) Real Estate Assessment Center (REAC) maintains and operates TASS. The primary goal of TASS is to utilize computer matching to identify potential areas of fraud, waste, and abuse in HUD's rental assistance programs. In support of this objective, TASS obtains tenant income information from the Social Security Administration (SSA), and two existing HUD systems – the Public and Indian Housing Information Center (PIC) and the Tenant Rental Assistance Certification System (TRACS).

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

Personal Identifiers:

X	Name:
X	Social Security Number (SSN):
	Other identification number (specify type):
X	Birth date:
X	Home address:
	Home telephone:
	Personal e-mail address:
	Fingerprint/ other "biometric":
	Other (specify):
	None
X	Comment: Administrators of HUD's rental assistance programs use this information to establish a family's initial and continued eligibility to participate in the programs and to correctly determine the level of subsidy the household is entitled to receive.

Personal/ Sensitive Information:

	Race/ethnicity:
	Gender:
	Marital status:
	Spouse name:
	Number of children:
X	Income/financial data (specify type of data, such as salary, Federal taxes paid, bank account number):
	Employment history:
	Education level:
	Medical history/information:
	Disability:
	Criminal record:
	Other (specify):
	None
X	Comment: Administrators of HUD's rental assistance programs use this information to establish a family's initial and continued eligibility to participate in the programs and to correctly determine the level of subsidy the household is entitled to receive.

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)?

	Yes
X	No
X	Comment: TASS is an existing system that is in the operational phase of its system development life cycle. PIH IT is conducting this initial PIA on the system in recognition of the importance of privacy protection and as part of its Department privacy best practices.

B. 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):

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 become 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 new 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 only a name and address)

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

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

Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
	Other (specify):
X	None

Rental Housing Assistance:

X	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, number of children, age)
	Property inspections
	Other (specify):
	None

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disburse funds to grantees – if any personal information is included
	Other (specify):
X	None

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
X	None

Internal Operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	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?

For example, another agency for a programmatic purpose or outside the government. Mark any that apply.

	Federal agencies (specify):
	State, local, or tribal governments
X	Public Housing Agencies or Section 8 property owners/agents
	FHA-approved lenders
	Credit bureaus
	Local and national organizations
	Non-profits
	Faith-based organizations
	Builders/developers
	Others (specify):
	None
X	Comment: Administrators of HUD's rental assistance programs use this information to establish a family's initial and continued eligibility to participate in the programs and to correctly determine the level of subsidy the household is entitled to receive.

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.
X	Comment: Administrators of HUD's rental assistance programs require this information to establish a family's continued eligibility to participate in the programs and to correctly determine the level of subsidy the household is entitled to receive. Opt-out is not possible if they wish to participate in HUD's rental assistance programs, but it is possible if they elect to withdraw from HUD's rental assistance programs.

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):_____N/A_____

_____

_____

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

Mark any that apply and give details if requested (if not applicable, mark N/A).

Yes	System users must log in with a password
Yes	When an employee leaves: PHAs are encouraged to terminate the user ID immediately.
Yes	Are access rights selectively granted, depending on duties and need-to-know? If yes, specify the approximate number of authorized users who have either: Full access rights to all data in the system (specify number) Approximately 10 PIH program personnel and 90 auditors from the HUD Office of Inspector General have full user access rights to the TASS system. Limited/restricted access rights to only selected data (specify number): Users roles are allocated according to their program and organization. Thus someone in a PHA would only see data relating to their PHA, a Housing program owner would only see data relating to their properties, a HUD employee in a Field Office would only see data for their program (housing or Public Housing) within the Field Office jurisdiction, etc. Housing program users: 15,000 PIH users: 5,000
Yes	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): Instructions (backed up by on-site audits) require that printouts and work products containing individual information be locked up when not in use.
Yes	If data from your system are 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: Data is extracted to a data warehouse used solely by PIH for management reports and for refinements and special runs of variants of existing TASS reports. Access to the data warehouse is strictly controlled by the TASS Headquarters User Administrator. All reports containing personal data will be marked on the top sheet "Warning: this report contains personal data. The only permitted uses are to assist in the re-certification process by Public Housing or in the oversight of that process." Following sheets will be marked at the top and bottom: "Warning: Privacy Act data. For use for governmental purposes only."
X	Comment: Unauthorized access is reduced by restricted access by job functions and the use of user IDs/ passwords. Servers are maintained in a secure data center and access is protected by firewalls. User sessions over the web are protected by the secure server (HTTPS protocol) with high-level encryption. File transfers for data processing are done using high-level encryption.

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

Mark any that apply.

X	Name:
X	Social Security Number (SSN):
	Identification number (specify type):
X	Birth date:
	Race/ethnicity:
	Marital status:
	Spouse name:
X	Home address:
	Home telephone:
	Personal e-mail address:
	None
X	Comment: The data elements that are retrieved are those necessary for income verification.

Other Comments (or details on any Question above):

SECTION 3. DETERMINATION BY HUD PRIVACY ADVOCATE

TASS provides information confirming the reasonableness of tenant reported income for households participating in HUD's assisted housing programs. The system does collect and retrieve personal/ sensitive information that's subject to the Privacy Act. As HUD's Privacy Advocate, I believe that there are adequate security controls in place for protecting this information, as outlined in Question 6 above. However, due to the vast amount of personal/ sensitive information contained in the system, we will **annually** monitor the system and its related business processes to ensure that this information is being safeguared.