U.S. Department of Housing and Urban Development

OFFICE OF HOUSING

Tenant Rental Assistance Certification System (TRACS)

Privacy Impact Assessment

April 2009

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Tenant Rental Assistance Certification System (TRACS)**. 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.

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/ James Legge 4/29/09
JAMES LEGGE, SYSTEM MANAGER **Date**
Office of Chief Information Officer
Office of Systems Integration and Efficiency

/s/ Lanier M. Hylton 4/29/09
LANIER M. HYLTON, PROGRAM AREA MANAGER **Date**
Office of Housing
Office of Program Systems Management

N/A
DEPARTMENTAL PRIVACY ADVOCATE **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

/s/ Donna Robinson-Staton 5/6/09
DONNA ROBINSON-STATON, DEPARTMENTAL PRIVACY ACT OFFICER **Date**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

TABLE OF CONTENTS

FINAL/APPROVED

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
"TENANT RENTAL ASSISTANCE CERTIFICATION SYSTEM (TRACS)"

(for IT Systems: 0025-00-01-03-01-1170-00-112-038
and Insert PCAS #: 00251780)

April 2009

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 Handbook1325.1 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?

The Program Area System Owner and IT Project Leader both 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 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 Housing
Subject matter expert in the program area: Lanier Hylton, Director, Office of Program Systems Management, (202) 708-0614 ext. 2510
Program Area Manager: Lanier Hylton, Director, Office of Program Systems Management (202) 708-0614 ext. 2510
IT Project Leader: James Legge, Computer Specialist, Office of the Chief Information Officer, Office of Systems Integration and Efficiency, (202) 402-7485; Jacqueline Miller, Director, Real Estate Management Division, Office of Systems Integration and Efficiency, (202) 708-0517

For IT Systems:

- **Name of system:** Tenant Rental Assistance Certification System (TRACS)
- **PCAS #:** 00251780
- **OMB Unique Project Identifier #:** 025-00-01-03-01-1170-00-112-038
- **System Code:** F87

For Information Collection Requests:

- **Name of Information Collection Request: Owner' Certification with HUD Tenant Eligibility and Rent Procedures**
- **OMB Control #:** 2502-0204

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

TRACS is the official repository for HUD's Multifamily Housing's assisted families including both current and historical data. Also, TRACS is the repository for tenant unit address and mailing address to support those HUD applications requiring the ability to locate the tenant's physical location or mail a document to their mailing address. TRACS collects and utilizes assistance contracting accounting and budgetary data from the HUD accounting financial systems, PAS/LOCCS and HUDCAPS.

The information is collected to improve fiscal control over Section 8 and other assisted housing programs at HUD. The goal of TRACS is to collect tenant data for all programs and automatically provide payment for subsidy programs where HUD is the contract administrator based upon the contract and tenant data resident in the system. The information will be used to process subsidy contracts and rental assistance information. Information is also used to verify the tenant eligibility for assistance and review the accuracy of the subsidy payment.

TRACS interfaces on a daily basis with trusted business partners responsible for carrying out the program mission and reporting program and performance data to TRACS. These entities are software vendors, Service Bureaus, local and state housing entities, Contract Administrators and private owners.

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:

X	Name
X	Social Security Number (SSN)
X	Other identification number (specify type): Alien Registration Number and Tax Identification Number (TIN)
X	Birth date
X	Home address
X	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
X	Comment: The information will be used to process subsidy contracts and rental assistance information. Information is also used to verify the tenant eligibility for assistance and review the accuracy of the subsidy payment.

Personal/ Sensitive Information:

X	Race/ ethnicity
X	Gender/ sex
	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.): tenant and qualifying household members income eligibility and recertification data; and State wage and claims data
X	Employment history:
	Education level
	Medical history/ information
X	Disability
	Criminal record
	Other (specify):
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	☒	☐
Have the security controls been reviewed and approved by the Information Security Officer?	☒	☐
What security controls are in place to protect the information (e.g., encryptions)? Encryption		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? TRACS is available through VPN. TRACS is accessed through HUD's secure systems connection front-end utilizing the Web Access Security Subsystem (WASS). HUD intranet users are validated with Microsoft Active Directory while internet users use LDAP (Lightweight Directory Access Protocol).		

Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department? Yes

HUD Policy: 5.2.17 (Handbook 2400.25)

a. The Deputy CIO for IT Operations shall provide remote access mechanisms that are centrally managed, monitored, and protected by strong authentication. The mechanisms shall have the capability to provide strong cryptographic mechanisms for authentication and protection of sensitive information during transmission. For access to moderate- or high-impact systems, the session shall be encrypted and access shall be managed through a limited number of managed access control point.

b. Program Offices/System Owners shall authorize and approve remote access methods for systems under their purview. The remote access methods shall only use mechanisms authorized by the Deputy CIO for IT Operations.

c. Remote access is limited to official use by individuals authorized by HUD management to work at home, or other non-HUD worksite, (e.g., maintenance ports and system and device administration) only for compelling operational needs and during emergencies.

d. ISSOs shall authorize in writing users requiring remote access, including remote access for privileged functions and documents the rationale for such access in the security plan.

e. Program Offices/Systems Owners of moderate- or high-impact systems shall use encryption to implement the following controls:

- Remote access
- Wireless access
- Cryptographic module authentication
- Transmission integrity and confidentiality

f. Program Offices/System Owners prohibited users from copying HUD-related documents to the hard/floppy drives of personally- or privately-owned computers. During the time a user is on the HUD telecommuting website, he or she is strictly prohibited from having an open peer-to-peer software connection (e.g., LimeWire, Napster, etc.) that enables internet file sharing, commonly used in the sharing of music files, with the Internet community at large.

Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Yes HUD Policy: 5.2.17 (Handbook 2400.25) f. Program Offices/System Owners prohibited users from copying HUD-related documents to the hard/floppy drives of personally- or privately-owned computers. During the time a user is on the HUD telecommuting website, he or she is strictly prohibited from having an open peer-to-peer software connection (e.g., LimeWire, Napster, etc.) that enables internet file sharing, commonly used in the sharing of music files, with the Internet community at large. HUD Policy: 5.2.20 (Handbook 2400.25) a. Program Offices/System Owners shall prohibit users from using personally- or privately-owned equipment and software (e.g., laptop computers, Blackberries, Universal Serial Bus (USB) flash drives, external drives, diskettes, removable media, or personal digital devices) to process, access, or store information for HUD-related work except through approved remote access or email without prior written approval from the Program Offices/System Owner. **c. HUD employees or contractors shall not transmit sensitive HUD information to any personal email account that is not authorized to receive it.** d. Program Offices/System owners shall prohibited users from downloading HUD-related work onto any external media from their HUD computer for the purpose of working on those documents or tasks on any personally or privately owned computer equipment.
Comment:

Question 3: Type of electronic system or information collection.

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	No
If yes, please proceed to answering the following questions.	☐	☒
Does the system require authentication?	☐	☐
Is the system browser-based?	☐	☐
Is the system external-facing (with external users that require authentication)?	☐	☐

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 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 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 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
X	No, the ICR does not require a PIA because it is not new or automated)
	Comment:

Question 4: 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):
	Comment:

Rental Housing Assistance:

X	Eligibility for rental assistance or other HUD program benefits
X	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

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

Mark any that apply:

X	Federal agencies? Social Security Administration (SSA), Health and Human Services (HHS)for the purpose of conducting computer matching activities as required by the Computer Matching and Privacy Protection Act of 1988, as amended
X	State, local, or tribal governments? Public Housing Agencies and Housing Finance Agencies
X	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): Software venders, Service Bureaus, local and state housing entities (i.e. Contract Administrators) private and owners
X	Comment: TRACS interfaces on a daily basis with trusted business partners responsible for carrying out the program mission (i.e., tenant and voucher payment) and reporting program and performance data to TRACS.

Question 6: 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): _____
_____

Question 7: 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	When an employee leaves: • How soon is the user ID terminated? (Access rights are terminated within 1 week of retirement and/or departure from HUD as part of the employee termination and/or retirement process.) MF Housing owners and agents are encouraged to terminate the user ID immediately. How do you know that the former employee no longer has access to your system? A request is sent to the System Administrator for the employee(s) removal from the system. Upon receipt of the request the System Administrator immediately removes the employee(s). In addition, the System Administrator annually recertifies employees. As part of re-certification, managers identify employees who no longer should have access because they have retired or transferred to new jobs.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system: none Limited/restricted access rights to only selected data: All users. Estimated between 15,000 – 20,000 are provided access based upon their duties. This project has a Security System Plan that was developed in accordance with OMB Bulletin 90-08 guidance and NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems. HUD's business partners for MF are the property owners and their agents . As a service to HUD's business partners, reports are downloadable, which contain tenant Privacy Act data, but it should be kept in mind that the identifiers are those known to the HUD business partners because they are the source of that data. There are technical controls in the computer system at HUD and physical safeguards provide security safeguards throughout the system of HUD and owner/agent community. Hence, HUD has minimal controls over the administrative safeguards at owner/agent sites and works to improve these controls throughout the user community of owner/agents that use the data.
X	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): Disk and tapes are secured and stored by Electronic Data Systems (EDS) at the computer site in Martinsburg, West Virginia. Printouts are currently secured in locked cabinets. As part of the future re-engineering of TRACS On-line filing will be integrated in the system for storage and retrieval of millions of contract and payment documents will increase efficiency and reduce storage and paper handling.
X	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: Tenant income data are transmitted to EIV. These data files are protected during transfer from TRACS to EIV in accordance to Security requirements requiring encryption of Privacy Act data. EIV use control points when receiving files (input control point) from TRACS. Program Administrators, Owners and Management Agents are responsible for protecting the data transmitted from TRACS.
	Other methods of protecting privacy (specify):
	Comment:

Question 8: If privacy information is involved, by what data elements is it retrieved?

Mark any that apply:

X	Name: Name of tenant and all house hold members, Name of owners/management agent
X	Social Security Number (SSN): Tenant/ owners/management agent
X	Identification number (specify type): Alien Registration Number and TIN
X	Birth date
X	Race/ ethnicity
	Marital status
X	Spouse name
X	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

TRACS is a concern for privacy protection due to the sensitive nature of the data collected and maintained by the system. Based on the responses provided for question #6 we have determined that adequate protection and security controls are in place for protecting the personal identifiable information housed by HUD and its Field Offices. The Privacy Program will review the PIA as system modifications are made to determine if the existing PIA warrants an update. MFH is

seeking OMB's review for an extension of the currently approved Information Collection Request (Q #3 of this PIA). The ICR will be renewed for an additional 3 year period and will expire in FY 2012. The information collected under the ICR by remains that same; therefore, there are no privacy impacts or concerns.