U.S. Department of Housing and Urban Development

OFFICE OF HOUSING

Tenant Rental Assistance Certification System (TRACS)

Privacy Impact Assessment
Version 4.2015

February 2016

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.

_____ **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.

SYSTEM OWNER **Win Chan, DIRECTOR (Acting)** Office of the Deputy Assistant Secretary for Multifamily Housing Program Systems Management Office	**Date**
CHIEF PRIVACY OFFICER OFFICE OF ADMINISTRATION	**Date**

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT.....2

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

1. Provide a general description of the system and answer the following questions to define the scope of the information in the system (or information collection). Specifically identify below the nature of the information collected and the sources from which it is obtained:.....7
2. Identify the type of system requirement being addressed by the PIA (If this is an Information Collection Request; items A, B and C are N/A)?.....8
3. Explain by Line of Business why the personally identifiable information is being collected. How will the information be used?.....9
4. Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?.....11
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)?.....11
6. How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....11
7. If privacy information is involved, by what data element(s) is it retrieved from the system?..... 12
8. What type of notice(s) is/are provided to the individual on the scope of the information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information?.....13
9. What are the Retention Use and Disposal Practices? Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.....13

SECTION 3 - DETERMINATION BY HUD PRIVACY Act officer.....14

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
["INSERT SYSTEM NAME"]

(for IT Systems: [Insert OMB Unique Identifier]
and [Insert PCAS #])

[Insert Date]

NOTE: See Section 2 for PIA answers, and Section 3 for the Chief Privacy Officer 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 superceded 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~~ **seven** 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 just 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 Officer in the Office of Administration.

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 Office of Administration, Office of the Executive Secretariat 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 Office of Administration, Office of the Executive Secretariat. If any question does not apply, state not applicable (N/A) and briefly explain why it is not applicable.

Program Area: Office of Housing
Subject matter expert in the program area: Lanier Hylton, Multifamily Housing Program Systems Management Office, (202) 402-2510
Program Area Manager: Lanier Hylton, Multifamily Housing Program Systems Management Office, (202) 402-2510 & Princess Martin, Multifamily Housing Program Systems Management Office, (202) 402-6093
IT Project Leader: LaShayla Hopkins, Computer Specialist, Office of the Chief Information Officer, Enterprise Program Management Division, (202) 402-5419;
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
- **Development Date:** In production
- **Expected Production Date:** In production

For Information Collection Requests:

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

1. **Provide a general description of the system and answer the following questions to define the scope of the information in the system (or information collection). Specifically identify below the nature of the information collected and the sources from which it is obtained:**

   A. What is the personal information being collected (e.g., name, address, gender/sex, race/ethnicity, income/financial data, employment history, medical history, Social number, tax identification number, employee identification number, FHA case number)? name, address, gender/sex, race/ethnicity, income/financial data, employment history, medical, Social number, tax identification number

   B. From whom is the information collected (i.e., government employees, contractors, or consultants)? The MFH Industry (owners/agents/contract administrators) submit the data to HUD regarding assisted tenants / households.

C. What is the functionality of the system and the purpose that the records and/or system serve? To provide rental assistance to specified MFH properties for very low/low income tenants.

D. How is the information transmitted to and from the system? Via a secure / encrypted file transfer system.

E. What are the interconnections with other systems? There are internal HUD interfaces to verify income (EIV), submit payment requests (EIV), validate contract / budget details and/or submit new funding transactions (PAS, HUDCAPS.) Please see the TRACS ICD for the complete list of interfaces.

1. WHAT SPECIFIC LEGAL AUTHORITIES, ARRANGEMENT, AND/OR AGREEMENT AUTHORIZE THE COLLECTION OF INFORMATION (I.E., MUST INCLUDE AUTHORITIES THAT COVER ALL INFORMATION COLLECTION ACTIVITIES, INCLUDING SOCIAL SECURITY NUMBERS)?

UNITED STATES HOUSING ACT OF 1937; AS AMENDED, 42 U.S.C. 1437 ET SEQ., AND THE HOUSING AND COMMUNITY DEVELOPMENT AMENDMENTS OF 1981, PUBLIC LAW 97-35, 95 STAT. 408.

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.

2. Identify the type of system requirement being addressed by the PIA (If this is an Information Collection Request; items A, B and C are N/A)**?**

A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)? N/A	**Yes** ☐	**No** ☐
Does the system require authentication?	☒	☐
Is the system browser-based?	☒	☐
Is the system external-facing (with external users that require authentication)?	☒	☐

B. If this is existing electronic system has the system undergone any changes (since April 17, 2003)**?** If an existing system, when was the system developed? Originally in 1992/1993 – though there have been extensive modifications._____	**Yes** ☒	**No** ☐
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	☐	☒
If yes, please explain:		

C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA or PIA update (if not applicable, mark N/A): 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)

	8. 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:

3. Explain by Line of Business why the personally identifiable information is being collected. How will the information 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)

4. Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?

Mark any that apply and give details if requested.

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, National Archives
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?
	HUD module/application? (specify the module(s)/application(s) name)
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

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. _____

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 (Please specify password type).

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? (explain your procedures or describe your plan to improve): 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 Hewlett Packard (HP) at the computer site in West Virginia. Printouts are currently secured in locked cabinets, as needed.
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:
Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated.	

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

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:

8. What type of notice(s) is/are provided to the individual on the scope of the information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information?

A. Was any form of notice provided to the individual prior to collection of the information? If yes, please provide a copy of the notice as an appendix.

(A notice may include a posted privacy policy, a Privacy Act notice on form(s), and/or a system of records notice published in the Federal Register.) If notice was not published, why not?

B. Do individuals have an opportunity and/or right to decline to provide information?
No

C. Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

9. What are the Retention Use and Disposal Practices? Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.

A. How long is information retained?

Data is retained in the system databases – both production and the archive. Files in iMAX are deleted via a standard quarterly procedure.

B. Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Data is provided to NARA

C. Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The data is maintained in a secure system – only users with authorized access are allowed.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER