

**U.S. Department of Housing and
Urban Development**

**Office of Policy Development and
Research**

**Policy and Research Information Server System
(PARIS) – P202**

Privacy Impact Assessment

February 2007

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Policy and Research Information Server (PARIS) – P 202**. 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/ Robert Gray

SYSTEM OWNER, ROBERT GRAY
Director, Program Monitoring & Research Division,
Office of Policy Development & Research

2/26/2007

Date

/s/ Seth Marcus

PROGRAM AREA MANAGER, SETH MARCUS
Social Science Analyst and ISSO

2/26/2007

Date

/s/ Jeanette Smith

**DEPARTMENTAL PRIVACY ACT OFFICER,
JEANETTE SMITH**
Office of Policy and E-Government, Office of the
Chief Information Officer

3/6/07

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?	5
When is a Privacy Impact Assessment (PIA) Required?	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT	7
Question 1: Provide a brief description of what personal information is collected.	7
Question 2: Type of electronic system or information collection.....	8
Question 3: Why is the personally identifiable information being collected? How will it be used?	9
Question 4: Will you share the information with others?	10
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)?	11
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?	11
Question 7: If privacy information is involved, by what data elements can it be retrieved?... ..	12
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	13

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
“POLICY AND RESEARCH INFORMATION SERVER (PARIS)”**

**(for IT Systems: [Insert OMB Unique Identifier (none – non-major)]
and PCAS #: 00309460)**

February 2007

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 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) (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 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

Program Area: Office of Policy Development and Research

Subject matter expert in the program area: Robert Gray, Director, Program Monitoring and Research Division, Office of Policy Development and Research, 202-402-5732

Program Area Manager: Seth Marcus, Social Science Analyst and ISSO, Program Monitoring and Research Division

IT Project Leader: Seth Marcus, Program Monitoring and Research Division, Office of Policy Development and Research, 202-402-6599

For IT Systems:

- **Name of system:** Policy and Research Information Server (PARIS)
- **PCAS #:** 00309460
- **OMB Unique Project ID:** None (non-major)
- **System Code:** P202

For Information Collection Requests:

- **Name of Information Collection Request:** n/a no information collected from public
- **OMB Control #:** n/a no information collected from public

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

PARIS/P202 provides research support (statistical analysis and database support). PARIS supports all HUD program offices by providing reliable data and analysis. PARIS is used for many research, evaluation, and reporting functions, such as responding to Congressional requests for data on assisted housing programs. PARIS does not collect personal identifiable information (PII); however, it does store and process PII that has been extracted from other upstream HUD systems (PIC and TRACS) that do collect PII. The data stored in the system is collected from Public Housing, Multifamily Assistance, and the Section 8 HCV program.

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

Personal Identifiers:

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

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
<input checked="" type="checkbox"/>	Gender/ sex
<input checked="" type="checkbox"/>	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Income sources and amounts (PIC and TRACS collects to determine program eligibility)
	Employment history:
	Education level
	Medical history/ information
<input checked="" type="checkbox"/>	Disability
	Criminal record
<input checked="" type="checkbox"/>	Other (specify): Type of public housing assistance
	None
	Comment:

Question 2: 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	Yes	No
	a. Does the system require authentication?	<input checked="" type="checkbox"/>	
	b. Is the system browser-based?		<input checked="" type="checkbox"/>
	c. Is the system external-facing (with external users that require authentication)?		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	No		
	Comment: P202 is only accessible to users authenticated on the HHQ LAN and who are authenticated by PD&R as established P202 users.		

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):

N/A	Conversion: When paper-based records that contain personal information are converted to an electronic system
N/A	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
N/A	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2:

	when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
N/A	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
N/A	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
N/A	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
N/A	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
N/A	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
N/A	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

(none of above are true)

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 <u>new</u> or <u>automated</u>)
	Comment: P202 does not directly collect PII data.

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

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:

	Eligibility for rental assistance or other HUD program benefits
X	Characteristics of those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
X	Comment: Data is stored in the system for the purpose of statistical analysis on participants in the Public Housing, Multifamily Assistance, and the Section 8 HCV program.

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):

X	Creation of Fair Market Rents, Income Eligibility Limits, and other benchmark statistics
X	Responding to Congressional inquiries (i.e. summaries of public housing tenants in a particular district or county)
X	Policy development, regulation changes, etc., based on verifiable research of tenant data. For instance, if research shows more disabled residents than accessible apartments, HUD may decide to change regulation of PHAs to increase # of accessible units.

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

X	Federal agencies? Data files are provided to the Census Bureau annually, and GAO for special studies, as permitted in the Privacy Act, Section 13.
X	State, local, or tribal governments? Summary data provided upon request

<input checked="" type="checkbox"/>	Public Housing Agencies (PHAs) or Section 8 property owners/agents? Summary data provided upon request
	FHA-approved lenders?
	Credit bureaus?
<input checked="" type="checkbox"/>	Local and national organizations? Summary data provided upon request
<input checked="" type="checkbox"/>	Non-profits? Summary data provided upon request
	Faith-based organizations?
	Builders/ developers?
<input checked="" type="checkbox"/>	Others? (specify): Researchers, academic institutions, organizations under contract with PD&R for research projects, and the public via www.huduser.org
<input checked="" type="checkbox"/>	Comment: We only share SUMMARY STATISTICS with others; we do not share raw data containing PII. We only post PUBLIC DATA FILES to the www.huduser.org website.

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
	No, they can’t “opt-out” – all personal information is required
<input checked="" type="checkbox"/>	Comment: n/a P202 does not COLLECT data. Data collection is handled by PIC and TRACS systems. We only receive quarterly extracts of PIC and TRACS data. Refer to the PIA for PIC and TRACS for details of how those systems collect data from the public and whether or not the public can opt-out.

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

<input checked="" type="checkbox"/>	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)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): Information is forwarded to the system administrator and the password is removed within one day. HUD LAN BRANCH and HUD IT SECURITY is responsible for terminating "H" and "C" login Ids on the HUD LAN.
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: YES – only system administrators (2) have full read/write access to system • Limited/restricted access rights to only selected data: YES – all regular users (about 80) have restricted rights – READ ONLY. <p>All PII data maintained with PARIS are strictly monitored and used only in accordance with our IT risk assessment, IT security plan, and the P202 Rules of Behavior, which all users agree to and sign. PARIS is only accessible to authorized PD&R users from within the HHQ domain, and is not available to the public.</p>
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? YES. No PII is written to disk or tape, or output to a printer. All PII remains securely stored in the Oracle databases.</p>
	<p>If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve:</p>
X	<p>Other methods of protecting privacy (specify): Refer to P202 System Security Plan.</p>
	<p>Comment:</p>

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

Since abstracts from PIC and TRACS are stored in the system, please let us know if these data elements are retrieved from the system.

	Name:
X	Social Security Number (SSN)
	Identification number (specify type):
X	Birth date
X	Race/ ethnicity
X	Marital status
X	Spouse name (head of household and, if present, co-head regardless of marriage status)
X	Home address
	Home telephone
	Personal e-mail address
X	Other (specify): Disability status

	None
X	<p>Comment: The data elements checked above are retrieved for the purposes of generating summary statistics. For instance, a member of Congress wants to know the race and ethnicity composition of public housing tenants in Cuyahoga County, OH (a very common type of request). We run a query of the Oracle data, selecting those elements for all tenants in that county. We then run summary statistical routines on those data elements and generate a summary table or chart, which is sent through HUD's Office of Congressional Relations to the Representative. The raw data containing PII remains in the Oracle database.</p> <p>Output from this system is also used in developing new policies and regulations, and for calculation of benchmark statistics such as annual Fair Market Rents and Income Eligibility Limits.</p>

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

Because of the personal identifiable information (PII) abstracts stored and processed by PARIS it is determined that a need to protect the data is warranted. Based on the information supplied for question #6 we have determined that the appropriate administrative controls are in place for protecting the PII. We will reevaluate the systems administrative controls as modifications are implemented to ensure that the current controls are still enforced.