

U.S. Department of Housing and Urban Development

Multifamily Housing

Active Partners Performance System (APPS) F24P

Privacy Impact Assessment

March 2007

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the **Active Partners Performance System (APPS)**. 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
[PROGRAM OFFICE]

Date

PROGRAM AREA MANAGER
[PROGRAM OFFICE]

Date

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

Date

DEPARTMENTAL PRIVACY ACT OFFICER
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

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.....	Error! Bookmark not defined.
Question 3: Why is the personally identifiable information being collected? How will it be used?	10
Question 4: Will you share the information with others?	11
Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?	12
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?	12
Question 7: If privacy information is involved, by what data elements can it be retrieved?...	13
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	14

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
ACTIVE PARTNERS PERFORMANCE SYSTEM (APPS) F24P
(for IT Systems: OMB Unique Identifier: N/A
and PCAS 00251460

March 2007

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Advocate's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- [Privacy Act of 1974, as amended](#) affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See <http://www.usdoj.gov/foia/privstat.htm>; see also [HUD Handbook 1325.1 at www.hudclips.org](#));
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See <http://www.usdoj.gov/foia/privstat.htm>);
- [Freedom of Information Act of 1966, as amended](#) (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also [HUD's Freedom of Information Act Handbook \(HUD Handbook 1327.1 at www.hudclips.org\)](#));
- [E-Government Act of 2002](#) requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- [Federal Information Security Management Act of 2002](#) (which superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security

regulations at [Title 44 U.S. Code chapter 35 subchapter II](http://uscode.house.gov/search/criteria.php) (<http://uscode.house.gov/search/criteria.php>); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

1. **New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).

2. Existing Systems: Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA): Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The [Privacy Act of 1974](http://www.usdoj.gov/foia/privstat.htm), as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The [E-Government Act of 2002](#) requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy 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 Advocate 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: Multifamily Housing

Subject Matter Expert: William Hill, Director, Policy and Participation Standards Division, Housing, (202) 708-1320 Ext. 2625

Program Area Manager: Same as Above

IT Project Leader: James E. Collins, Management Analyst, Policy and Participation Standards Division, Housing, (202) 708-1320 Ext. 3279; Veronica Quander, Director, Real Estate Assessment Division (202) 748-5495 Ext. 2477

For IT Systems:

- **Name of system:** Active Partners Performance System (APPS)
- **PCAS #:** 000251460
- **OMB Unique Project Identifier #:** N/A APPS is under the iREMS system whose number is HSG - 1768000
- **System Code:** F24P

For Information Collection Requests:

- **Name of Information Collection Request:** N/A
- **OMB Control #:** N/A

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

The APPS Registration Page requires coordinators/users to enter their Organization or Individual Name, SSN or TIN #, Type of Organization, Legal Structure, Address, Phone and Email information.

The User ID maintenance actions are performed via the WASS system which collects and processes User ID's based on information gathered from the APPS registration page or existing information in REMS and generates access key codes for Individuals/Companies. Users have to enter valid User ID's and Passwords via Secure Systems to get into APPS.

Within the APPS system Social Security Number (SSN) and Tax Identification Number (TIN) are used as the identifier for Individuals/Companies to enter their previous participation information in the system so that they can complete necessary procedures and apply to participate in HUD properties.

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): Individual Taxpayer Identification Number (TIN)
N/A	Birth date
X	Home address
X	Home telephone
X	Personal e-mail address
N/A	Fingerprint/ other "biometric"
N/A	Other (specify):
N/A	None
N/A	Comment:

Personal/ Sensitive Information:

N/A	Race/ ethnicity:
N/A	Gender/ sex:
N/A	Marital status:
N/A	Spouse name:
N/A	# of children :
N/A	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.) :
N/A	Employment history:
N/A	Education level:
N/A	Medical history/ information:
N/A	Disability:
N/A	Criminal record
N/A	Other (specify):
N/A	None
N/A	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed? If yes, what security controls are in place to protect the information e.g., encryptions (give details below)?

Yes	No	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	If yes, have the security controls been reviewed and approved by the Information Security Officer?
		Not applicable, no personally identifiable information is collected in the system.

	Comment: APPS is a web-based system. Personally identifiable information is accessed remotely by authorized users via Secure System WASS.
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------

Question 3: 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	No	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. Does the system require authentication?
<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. Is the system browser-based?
<input checked="" type="checkbox"/>	<input type="checkbox"/>	c. Is the system external-facing (with external users that require authentication)?
		Comment:

A. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (if not applicable, mark N/A):

<input checked="" type="checkbox"/>	Conversion: When paper-based records that contain personal information are converted to an electronic system
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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)
<input checked="" type="checkbox"/>	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)
<input checked="" type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
<input type="checkbox"/>	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data

X	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.

X	Yes, this is a new ICR and the data will be automated
N/A	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>
N/A	Comment:

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

Mark any that apply:

Homeownership:

X	Credit checks (eligibility for loans)
X	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
X	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
X	Loan default tracking
N/A	Issuing mortgage and loan insurance
X	Other (specify): Rating and Ranking individuals who participate in Multifamily Housing projects.
N/A	Comment:
N/A	
N/A	

Rental Housing Assistance:

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

Grants:

N/A	Grant application scoring and selection – if any personal information on the grantee is included
N/A	Disbursement of funds to grantees – if any personal information is included

N/A	Other (specify):
N/A	Comment:

Fair Housing:

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

Internal operations:

N/A	Employee payroll or personnel records
N/A	Payment for employee travel expenses
N/A	Payment for services or products (to contractors) – if any personal information on the payee is included
N/A	Computer security files – with personal information in the database, collected in order to grant user IDs
N/A	Other (specify):
N/A	Comment:

Other lines of business (specify uses):

N/A	
N/A	
N/A	

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

Mark any that apply:

X	Federal agencies?
X	State, local, or tribal governments?
X	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
N/A	FHA-approved lenders?
N/A	Credit bureaus?
N/A	Local and national organizations?
N/A	Non-profits?
N/A	Faith-based organizations?
N/A	Builders/ developers?
N/A	Others? (specify):
N/A	Comment:

Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

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

Mark any that apply and give details if requested:

X	System users must log-in with a password
X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? <ul style="list-style-type: none"> ○ APPS Is not responsible for User ID Maintenance. The Coordinators for the Business Entities can terminate a User effective immediately. ○ For Internal users System access is removed within one business day of notification by the employee’s supervisor, a HUD GONE request, or a request from management. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): As stated above.
X	<p>Are access rights selectively granted, depending on duties and need-to-know? HUD users are given access according to their duties. The Business level entities chose their coordinators and have to request formal authorization to view or modify any information in APPS for a user.</p> <p>If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> • Internal HUD users 2538 • External Industry Users - 8069
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): Under the current paper process the personal information is locked up in cabinets at HUD HQ and locked inside a locked room inside another looked room. The</p>

	Automated information is in the APPS system which need passwords to gain access. APPS has been enhancing security and only displaying the last 4 digits of the SSN/TIN #'s in the system.
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: The automated information is shared with other multifamily systems such as. All the multifamily systems use WASS Secure Systems to be able to access the individual systems. User ID's and passwords are required to get passed Secure Systems. WASS is responsible for protecting this information. The system provides secure connection, identification and authorization services, please refer to the WASS PIA for additional information
N/A	Other methods of protecting privacy (specify):
N/A	Comment:

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

Mark any that apply:

X	Name:
X	Social Security Number (SSN) TAX ID
X	Identification number (specify type): ITIN
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
X	Home telephone
X	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

Due to the personally identifiable information (PII) collected and maintained by APPS, the system is a Privacy concern. Based on our observations the system does have adequate administrative controls to assure protection of PII. User ID's and passwords are administered to gain access to the PII information and access to this information is restricted to only those persons with a business need-to-know in the official capacity of their job duties. Business entities only have access to their specific data and must request formal authorization to review and/or modify their data. All users to the system are authenticated through the WASS secure connection, identification and authorization services. A Privacy Act System of Record Notice (SORN) is required for this system. To visit this SORN in text form, please visit: <http://www.hud.gov/offices/cio/privacy/documents/records.pdf>