

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

Office of Chief Financial Officer

**Audit Resolution and Corrective Actions Tracking
System (ARCATS)**

Privacy Impact Assessment
Version 3.2013

February 28, 2014

DOCUMENT ENDORSEMENT

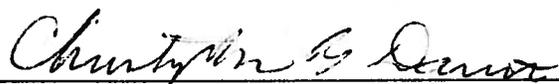
I have carefully assessed the Privacy Impact Assessment (PIA) for the Audit Resolution and Corrective Actions Tracking System (ARCATS). This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact 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.



Christopher B. Davies
Acting Assistant Chief Financial Officer for Systems
Office of the Chief Financial Officer
U.S. Department of Housing and Urban Development

2/28/14
Date



Simin D. Narins
Director, Financial Systems Quality Assurance Division
Office of the Chief Financial Officer
U. S. Department of Housing and Urban Development

2/28/14
Date



Donna Robinson-Staton
Departmental Privacy Act Officer
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

3/7/14
Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	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 general description of the system that describes: The following questions are intended to define the scope of the information in the system (or information collection), specifically the nature of the information and the sources from which it is obtained.....	7
Question 2: Type of electronic system or information collection.	8
Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?	10
Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)? No...11	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)?.....11	11
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 element(s) is it retrieved from the system?	14
Question 8: What type of Notice(s) are provided to the individual on the scope of information collected, the opportunity to consent to uses of said information, the opportunity to decline to provide information.	14
Question 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.	15
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....	16

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
AUDIT RESOLUTION AND CORRECTIVE ACTIONS TRACKING SYSTEM
(ARCATS)**

**(for IT Systems: Not a Major System therefore an Exhibit
OMB 300 was not submitted to OMB
and PCAS #360690)**

February 28, 2014

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 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>); 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 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 the Chief Financial Officer / Audit Liaison Division

System Owner: Christopher Davies, Acting Assistant Chief Financial Officer for Systems, Office of the Chief Financial Officer, (202) 402-3758

Subject Matter Expert in the Program Area: Kathryn Nicholson, Audit Liaison Division, Office of the Chief Financial Officer, HUD, (202) 402-3902

IT Project Leader: Christopher L. Turner, Office of Systems Integration & Efficiency, Office of the Chief Information Officer, (202) 402-7126; Harry Laggah, Office of the Chief Information Officer, HUD, (202) 402-6842

For IT Systems:

- **Name of system:** Audit Resolution and Corrective Action Tracking System (ARCATS/P136)
- **PCAS #:** 360690
- **System Code:** P136
- **Development Date:** Starting January 2014
- **Expected Production Date:** December 2014

For Information Collection Requests:

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

Question 1: Provide a general description of the system that describes: The following questions are intended to define the scope of the information in the system (or information collection), specifically the nature of the information and the sources from which it is obtained.

- a. What is the personal information being collected?** The system contains the following information: name, social security number, birth date, home address, home telephone, e-mail address, race/ethnicity, gender, marital status, spouse name, number of children, income/financial data, employment history, education level, medical history, and disability information.

The PII is contained in attachments only. The attachments may or may not have PII data in it. There is no specific field in ARCATS that collect this data.

- b. From whom is the information collected (i.e., government employees, contractors, or consultants)?** Information is collected by HUD employees and the Office of the Inspector General (OIG) from auditees.

- c. What is the functionality of the system and the purpose that the records and/or system serve?** The existing ARCATS system is a Lotus Notes based system, utilized within the Department to track and monitor Audits and Recommendations issued by the Office of the Inspector General (OIG), the Government Accountability Office (GAO), and single audit act auditors. The System also serves as the principle electronic tool to journalize the resolution of audit recommendations. The Lotus Notes platform ARCATS resides on is antiquated and unsupported. In FY14 ARCATS will be migrated from the Lotus Notes Platform to the AINS, eCase platform, a configurable COTS product for which HUD has obtained an enterprise license. This PIA will cover the ARCATS development effort. Once the ARCATS development is complete, this PIA will be updated to reflect the production environment of ARCATS.
- d. How information is transmitted to and from the system?** HUD and OIG employees can input text or upload files directly into the system.
- e. What are the interconnections with other systems?** N/A
- f. 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)?**
- Federal Managers Financial Integrity Act of 1982 (Pub. L. 97-255, HR 1526)
 - Sec. 113 of the Accounting and Auditing Act of 1950 (31 U.S.C. 66a)
 - ARCATS has been designed to conform with the requirements of the Inspector General Act of 1978 as amended (5 USC APP. 3), Office of Management and Budget (OMB) Circular A-50 revised "Audit Follow-up" and OMB Circular A-133 "Audits of States, Local Governments, and Non-Profit Organizations."

Question 2: Type of electronic system or information collection.

	Yes	No
A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Does the system require authentication?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

	Yes	No
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? January 2014	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Do the changes to the system involve a change in the type of records	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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	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)

D. 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
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>
✓	N/A

Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

<input type="checkbox"/>	Credit checks (eligibility for loans)
<input type="checkbox"/>	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
<input type="checkbox"/>	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
<input type="checkbox"/>	Loan default tracking
<input type="checkbox"/>	Issuing mortgage and loan insurance
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Rental Housing Assistance:

<input type="checkbox"/>	Eligibility for rental assistance or other HUD program benefits
<input type="checkbox"/>	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
<input type="checkbox"/>	Property inspections
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Grants:

<input type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Fair Housing:

<input type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Internal operations:

<input type="checkbox"/>	Employee payroll or personnel records
<input type="checkbox"/>	Payment for employee travel expenses
<input type="checkbox"/>	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):

✓	Reference for the OIG/HUD in support of audit resolution. Electronic storage/paperless environment as mandated by the Paperwork Reduction Act.
---	--

Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)? No.

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	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)
	Others? (specify):
✓	N/A

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

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:

✓	System users must log-in with a password (Please specify password type)
✓	<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)? Users are removed from all HUD Systems as soon as the Office Technology Coordinator (OTC) is contacted to prepare "HUD Gone" which usually takes one 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): If system access is disabled, the user will not be able to log on to HUD Domain.
✓	<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: Only Audit liaison officers, AINS contractors and Highland contractors have full access rights to all the data in the system. This is subject to change, as the system is currently in development. • Limited/restricted access rights to only selected data: Each attachment is limited to the action official, recommendation action official, program point of contact, audit liaison officer, relevant OIG staff, and other specifically identified HUD individuals specifically assigned to the recommendation the attachment is associated with. This is the target; however, it is subject to change, as the system is currently in development.
✓	<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): For the migration, the ARCATS database will be transported to AINS via the HITS provided encrypted hard drive. For future day-to-day operations, all confidential information, disks, tapes and printouts containing personal information is stored in key-locked cabinets.</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>
✓	<ul style="list-style-type: none"> • Other methods of protecting privacy (specify): Document Attachments containing sensitive, private information are marked private and are only accessible to personnel assigned to that particular recommendation or those specifically added to the read access control by the person entering the data into the system.
	<p>Comment:</p> <p>Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated. There is a privacy risk in terms of the disclosure of sensitive information to unauthorized people. The risk of collecting/maintaining SSN and other PII is that it can be misused or disclosed for an unauthorized purpose. To mitigate this risk, access to the system is limited to those who</p>

have a business need to know. Users have limited access that is established based on their role. Audit liaison officers and AINS and Highland contractors have full access rights to all the data in the system. This is subject to change, as the system is currently in development.

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

Mark any that apply

	Name:
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
✓	None
✓	<p>Comment: There are no specific data fields in the system for any of these. The information is contained inside attachments only.</p> <p>The information has nothing to do with HUD employees. The information is contained in attachments only, as there are no data fields in the system for the data. There is no file identifier. The attachment can only be pulled up when you are in the specific audit it is attached to and you must be one of the persons identified as able to see it. For example: if someone goes into a specific recommendation's action plan to close it, he/she then looks to see if there is an attachment (which there may or may not be) that contains closure information. This closure information attachment may or may not have PII data in it. The attachments with PII are marked as private by the person adding it into the system. There are no reports or searches available to find attachments marked private.</p>

Question 8: What type of Notice(s) are provided to the individual on the scope of information collected, the opportunity to consent to uses of said information, the opportunity to decline to provide information.

- a. Was any form of notice provided to the individual prior to collection of 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? A system of records was published in the Federal Register on February 6, 2013. The SORN will be modified when ARCATS enters production.
- 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?** No.

Question 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?**

Retention and disposal is in accordance with Records Disposition Schedule 21, HUD Handbook 2225.6. Records are destroyed or deleted when no longer necessary for agency business in accord with applicable federal standards or in no less than seven years after last action in accord with limitations on civil actions by or against the U.S. Government (28 U.S.C. 2401 and 2415).

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

Yes.

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

Risks associated with data retention for ARCATS include the possibility of data being accessed by unauthorized personnel and compromised PII (Personally Identifiable Information). Risks to the data in ARCATS are mitigated through the use of system scans, testing, and reviews.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Audit Resolution and Corrective Action Tracking System (ARCATS) P136 is a concern for privacy due to the personal/sensitive information contained in the system. Based on Question #6, we have determined that the appropriate administrative controls are in place to ensure protection of the data collected and maintained by the system. Approval of this assessment is recommended and that the review and/or update of the PIA for P136 required by July 28, 2015. Note: The ATO for this system expires in March 2014, recommend that you schedule a follow-up with IT Security.