

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

**Office of Multifamily Housing
And
Office of Healthcare Programs**

**Application Submission and Processing
System
(ASAP/P280)**

**Privacy Impact Assessment
Version 3**

July 23, 2014

DOCUMENT ENDORSEMENT

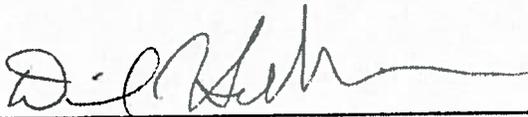
I have carefully assessed the Privacy Impact Assessment (PIA) for **Application Submission and Processing (ASAP – P280)**. This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (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.

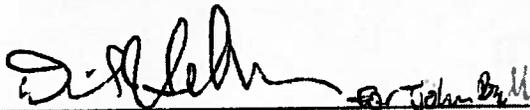
Based on our authority and judgment, the data captured in this document is current and accurate.



DANIEL J. SULLIVAN, SYSTEM OWNER
Deputy Director, Multifamily Development, Housing
Policy Division, U. S. Department of Housing and Urban
Development

8/18/14

Date



JOHN C. BELL, PROGRAM AREA MANAGER
Housing, Technical Support Division, U. S. Department
of Housing and Urban Development

8/18/14

Date



**PRINCESS MARTIN, SENIOR PROGRAM
MANAGER**, Office of the DAS for Multifamily
Housing Programs, U.S. Department of Housing &
Urban Development

8/19/14

Date



**DONNA ROBINSON-STATON, CHIEF PRIVACY
OFFICER**, Office of the Chief Information Officer,
Privacy Office, U.S. Department of Housing and Urban
Development

8/20/14

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	2
PLEASE CHECK THE APPROPRIATE STATEMENT.....	2
THE DOCUMENT IS ACCEPTED.....	2
THE DOCUMENT IS ACCEPTED PENDING THE CHANGES NOTED.....	2
THE DOCUMENT IS NOT ACCEPTED.....	2
SYSTEM OWNER.....	ERROR! BOOKMARK NOT DEFINED.
PROGRAM AREA MANAGER.....	2
DEPARTMENTAL PRIVACY ACT OFFICER.....	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 2: Type of electronic system or information collection.....	9
Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?	11
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)?.....	12
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)?.....	13
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	13
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	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.....	17

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
Application Submission and Processing
(ASAP/P280)**

(for IT Systems: 025-00-01-04-01-1810-00 and PCAS: 633990)

July 23, 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 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 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, as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Act Officer in the Office of the Chief Information Officer (OCIO). If any question does not apply, state **Not Applicable (N/A)** for that question, and briefly explain why it is not applicable.

Program Area: Office of Housing

System Owner/Contact information: Daniel Sullivan (202)-402-6130

Sr. Program Manager/Contact: Princess Martin (202) 402-6093

Program Area Functional Manager: John C. Bell (202) 402-2740

IT Project Manager/Contact Information: Cherri L. Mizelle (202) 402-3338

For IT Systems:

- **Name of system: Application Submission and Processing (ASAP)**
- **PCAS #: 633990**
- **OMB Unique Project Identifier #:**
- **System Code: P280**
- **Development Date: 9/2013 – January, 2015 (Target/Planned) for Initial Operating Capability (IOC)**
- **Expected Production Date: January 31, 2015**

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

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?

Project Files/records in the system for every Multifamily and Healthcare project will contain the following information: Mortgagee's/Borrower's names and names of principals and those of designated principals including that individual's, Employee identification Number/Tax Identification Number, Project name, project sponsor's Name, Project Number, Account Number, and Unit Address. Various required HUD forms collect the above personal information at the project-level from business partners and contractors for the purpose of obtaining mortgage insurance for HUD Multifamily Housing and Healthcare Projects.

- b. From whom is the information collected (i.e., government employees, contractors, or consultants)?**

The information is collected from both the internal and external parties including the U.S. Department of Housing and Urban Development headquarters and production center staff, and external business partners. The external business partners are Mortgagees (HUD approved Multifamily Accelerated Processing (MAP) and Healthcare Lenders). Multifamily MAP and Healthcare approved Lenders nationwide will have limited access to only their individual submission packages.

- c. What is the functionality of the system and the purpose that the records and/or system serve?**

The ASAP system is an automated FHA mortgage insurance application processing system that supports processing, tracking and underwriting of Multifamily Housing (MFH) and its Healthcare (OHP) program applications. The system will be designed to support underwriting of applications submitted to HUD by approved lenders for FHA insurance for the above mentioned programs. It will help to increase the sharing of information throughout MFH and OHP making the process more efficient, accurate, and transparent, thereby improving the partner relationships with both internal and external parties. Currently, the applications process relies heavily on manual processing of paper forms and documents with some staff manually inputting data into the DAP (Development Applications Processing) system which meets the needs of the tracking of the pipeline data at a minimum for MFH. The new system is expected to provide an end-to-end solution from Concept phase to final closing for MFH, and will align with the OHP process improvement for both the Office of Residential Care Facilities (ORCF) Section 232 program and The Office of Hospital Facilities (OHF) Section 242 programs that provide access to quality healthcare and residential facilities.

This ASAP project initiative will provide an improved way of managing the pipeline data and electronic processing of the lender applications benefiting both MFH and OHP. This fully integrated solution allows electronic submission of application using a web portal, provides enhancement to reporting capabilities, and document management solutions. Upon full implementation, this new system will replace in its entirety the MFH DAP system.

- d. How information is transmitted to and from the system?**

Mortgagees (HUD-approved Multifamily MAP or Healthcare Lenders) will electronically submit application package for these projects. Data will also be derived from various HUD-required forms. Other data is electronically submitted

by HUD source systems: Integrated Real Estate Management System, HEREMS, the Online Property Integrated Information Suite, and Subsidiary Ledger.

e. What are the interconnections with the other systems?

The new ASAP will interface directly with the integrated Real Estate Management System (iREMS/F24) and the HEREMS database. It will also interface with the Lender Electronic Assessment Portal – Institution Manager (LEAP-IM/P278) and the HSG Multifamily On-Line Property Integrated Information Suite Data Mart (HM-OPIIS/P220). Future interfaces with the ASAP may include FHA Subsidiary Ledger (FHA-SL/P013), and the Capital Needs Assessment Alignment (CNA-IT), and other systems.

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)?

HUD is authorized to collect the social security number (SSN) by Section 165(A) of the Housing and Community Development Act of 1987, P.L 100-242 and by 42 U.S.C. 3543.

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 checked="" type="checkbox"/>	<input 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? <u> N/A </u>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>
If yes, please explain:		

<p>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):</p>	
N/A	<p>Conversion: When paper-based records that contain personal information are converted to an electronic system. Target for conversion to the new system, replacing the legacy application system, is January 2015.</p>
N/A	<p>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</p>
N/A	<p>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)</p>
N/A	<p>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)</p>
X	<p>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)</p>
N/A	<p>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)</p>
N/A	<p>New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA</p>
X	<p>Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data The business process for how multifamily housing operates was recommended a new business process flow that has been incorporated in the configuration of the new ASAP. The recommendation included HUD move to using a commercial-of-the-shelf (COTS), industry standard approach for modernizing our business that would allow for increased efficiencies, improved data accuracy and availability, and better risk and fraud management for both the Multifamily Housing and Healthcare Programs. The production implementation target date is January 31, 2015.</p>
N/A	<p>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)</p>

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.

X	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>)
	Comment:

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

Mark any that apply:

Homeownership or Rental Housing Finance:

X	Credit checks (eligibility for loans)
X	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
X	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

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

Grants:

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

Fair Housing:

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

Internal operations:

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

Other lines of business (specify uses):

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

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	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):
X	Comment: Information will be shared only with the approved HUD Headquarter and field offices. Mortgagees (HUD approved Multifamily MAP or Healthcare Lenders) will only be able to view/access their own submission packages.

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.
X	No, they can’t “opt-out” – all personal information is required
	Comment:

If yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): _____

Question 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	<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)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): • Access is deleted from the main HUD Servers via the HUD separation form and upon notification by Supervisor, access is deleted/de-activated from DAP. <p>Access to the server happens immediately upon termination from the government. Once access is denied to the servers, these users no longer have access to any internal HUD system. ASAP is an internal HUD system. Deletion from the system usually happens within one week of departing the government or upon notification by Supervisor.</p>
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: Full access rights will be limited to HUD employees only. <p>Limited/restricted access rights to only selected data: Multifamily MAP and Healthcare approved Lenders nationwide will also have access to the system but will have limited access to only their individual submission packages.</p>
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):</p> <p>Electronic files are stored on disc and back up files are stored on tape. Printed/hard copies are stored and maintained in accordance with the applicable Multifamily or Healthcare records retention policies.</p>

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: An Interface Control Document (ICD) shall be documented and signed by all shared system owners.
X	Other methods of protecting privacy (specify): Multifamily MAP and Healthcare approved Lenders nationwide will also have access to the system but will have limited access to only their individual submission packages.
	Comment:
	Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated.

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)
X	Identification number (specify type): Project #, or project status
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
X	Comment: Information can only be retrieved via the project number or the project status. Access rights to specific personal information are only provided to HUD users with rights to the Underwriting portion of the system. Multifamily MAP and Healthcare approved Lenders nationwide will also have access to the system but will have limited access to only their individual submission packages.

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 and 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?**

Yes. As per the HUD Office of Chief Information Officer's Project Planning methodology Version 1.0, the System of Records Notice (SORN), was prepared and submitted during the Design phase. Federal Register to be published on the replacement system for the existing development application system has been prepared and submitted by the Office of Housing, MFH Programs and the Office of Healthcare programs for review to the OCIO. (July 2014)

- b. **Do individuals have an opportunity and/or right to decline to provide information?**

No, individuals can't "opt'out" – all information is required.

- 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?**

ASAP retention and disposal procedures are in accordance with approved General Service Administration schedules of retention and disposal included in HUD's Handbook 2228.2, appendix 14, items 21-26. Electronic and hard copy records will be retained between 10 and 40 years depending on financial terms. Afterwards, electronic records are purged or deleted from the system when eligible to be

destroyed using one of the methods described by the NIST SP 800-88 "Guideline for media Sanitization" (September 2006). Paper based records when eligible to be destroyed will be destroyed by shredding or burn. **NOTE:** Upon full implementation of new ASAP system, paper copy records will no longer be produced. The paper copies that existed under the prior manual system process will have be uploaded into the new system format, and official documentation will have been archived to the designated facility and destroyed when eligible to be destroyed.

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

Records will be retained and disposed of in accordance with the General Records Schedule included in HUD Handbook 2228.2, appendix 14, items 21-26. Paper base records are destroyed by burn or shredding. **NOTE:** Upon full implementation of new ASAP system, paper copy records will no longer be produced. The paper copies that existed under the prior manual system process will have be uploaded into the new system format, and official documentation will have been archived to the designated facility and destroyed when eligible to be destroyed.

Electronic records are purged or deleted from the system when eligible to be destroyed using one of the methods described by the NIST SP 800-88 "Guideline for media Sanitization" (September 2006).

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

Strict access controls are governed for electronic records by the use of a user ID and password that require authentication before access is granted to ASAP. All printed/hard copies that currently exist for projects will need to be created and stored in each HUD office in locked file cabinets when not in use, which access is limited to those personnel who service the records. **NOTE:** Upon full implementation of ASAP, hard copies will no longer exist for the new system. Paper records that existed under the prior manual process will have been uploaded into the new system format for electronic safeguarding. Records that existing under the prior manual process will have be shipped to the designated storage and archive facility who will safeguard the records in accordance with Departmental safeguarding procedures and policies.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Privacy Office examined the Multifamily Application Submission and Processing System (ASAP/P280) PIA responses and has determined that there are no privacy related risks at this time. If decisions change concerning the collection of PII the program sponsor will consult with Privacy Office to ensure that all privacy related requirement are addressed. This is a Privacy Sensitive PII system but it is not a candidate for the minimization of SSNs due to the fact that the information of necessary to provide services and the information is not retrieved from the system via SPII. The SORN is required at this time. The Program Office will re-certify the IPA NLT January 10, 2017, in compliance with the FISMA requirements. Approval of this assessment is recommended.

