

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

**Office of Lender Activities and Program
Compliance
Office of Single Family Housing**

**Lender Electronic Assessment Portal
LEAP – P278**

Privacy Impact Assessment
Version 3.2013

March 20, 2014

DOCUMENT ENDORSEMENT

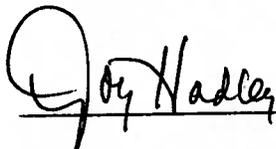
I have carefully assessed the Privacy Impact Assessment (PIA) for [Insert Name of IT System and/ or Information Collection Request]. This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

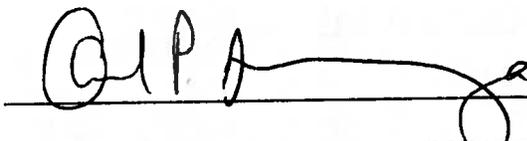
- The document is accepted.
 The document is accepted pending the changes noted.
 The document is not accepted.

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



**JOY HADLEY, DIRECTOR
OFFICE OF LENDER ACTIVITIES AND
PROGRAM COMPLIANCE, OFFICE OF
SINGLE FAMILY HOUSING**

14 Apr 2014
Date



**DANIEL SZPARAGA, INFORMATION
SPECIALIST
OFFICE OF LENDER ACTIVITIES AND
PROGRAM COMPLIANCE, OFFICE OF
SINGLE FAMILY HOUSING**

4/14/2014
Date



**DEPARTMENTAL PRIVACY ACT OFFICER
Donna Robinson-Staton
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development**

5/1/2014
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.....	ERROR! BOOKMARK NOT DEFINED.
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?	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)?.....	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 element(s) is it retrieved from the system?.....	13
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.....	14
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....	15

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
LENDER ELECTRONIC ASSESSMENT PORTAL (LEAP / P278)**

OMB Unique Identifier TBD, PCAS # 00663990 - HSG-663990-FHA Transformation

March 20, 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?

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 Lender Activities and Program Compliance, Office of Single Family Housing

Subject Matter Expert in the Program Area: Volky Garcia

Program Area Manager: Joy Hadley

IT Project Leader: Daniel Szparaga

For IT Systems:

- **Name of system:** Lender Electronic Assessment Portal (LEAP)
- **PCAS #:** 00663990 - HSG-663990-FHA Transformation
- **OMB Unique Project Identifier #:** TBD
- **System Code:** P278
- **Development Date:** Spring 2011 – Spring 2014
- **Expected Production Date:** May 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.

- What is the personal information being collected?** (e.g. name, address, gender/sex, race/ethnicity, income/financial data, employment history, medical history, Social Security Number, Tax Identification Number, Employee Identification Number, FHA Case Number): Name, address, employment history, Social Security Number, credit reports for individuals who have designated leadership roles at firms that are HUD's business partners; Tax Identification Number and bank account numbers for firms that are HUD's business partners.
- From whom is the information collected (i.e., government employees, contractors, or consultants)?** Private sector firms who are FHA's business partners.
- What is the functionality of the system and the purpose that the records and/or system serve?** Serving as the system of record for lenders working with HUD's Office of Housing, processing applications from lenders seeking approval to originate FHA-insured mortgages, monitoring the ongoing compliance of these

firms with HUD requirements once approved, monitoring changes in risk that these firms may present to the agency over time and ensuring that the business interface between these firms and the agency are optimally aligned and efficient. These are not new activities for the agency. Rather, HUD is migrating current functionality and data from existing systems and platforms onto a single platform in order to attain operational efficiencies.

d. How information is transmitted to and from the system: Information is manually uploaded by business partners or transferred through interfaces with other HUD and government IT systems.

e. What are the interconnections with other systems. LEAP is a replacement system for both IMF / F51 and LASS / P096. As such, it inherits their interfaces. Version 3.0 of LEAP does away with the LEAP-to-IMF interface since it does away with IMF. LEAP will have interfaces with the following systems:

- GSC – A15
- SFIS – A43
- CLAIMS – A43C
- SFNW – A80W
- SFPCS-P – A80B
- SFPCS-U – A80R
- SAMS – A80S
- SFDW – D64A
- CHUMS – F17
- FHA Connection – F17C
- SFDMS – F42D
- ARRTS – F51A
- CAIVRS – F57
- Title I Insurance and Claims – F72
- FHASL – P013
- NTHHQ – P16 (the Lender List functionality on the HUD.GOV portal)

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)? The system will collect and store name, addresses and SSN for key principals of HUD's lending business partners. Credit and background investigations are conducted which may result in the collection of PII. Resumes may be obtained. Authorization for collecting this data can be found in Title I and Title II of the National Housing Act; 12 U.S.C. 1703, 1709 and 1751b; 42 U.S.C. 1436(a) and 3535(d).

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>First rolled out May 2012.</u>	<input checked="" 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 checked="" type="checkbox"/>
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
Y	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)
Y	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)
Y	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 <u>new</u> Request that will collect data that will be in an <u>automated</u> 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 <u>new</u> request and the collected data will be in an <u>automated</u> 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>)
	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:

	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
	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):

X	Lender application for FHA's mortgage insurance program – compliance with law and policy for initial eligibility
X	Lender recertification – compliance with law and policy for continued eligibility
X	Credit checks (suitability of lender principals)

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)?

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?
X	HUD module/application? (specify the module(s)/application(s) name) GSC – A15, SFIS – A43, CLAIMS – A43C, SFNW – A80W, SFPCS-P – A80B, SFPCS-U – A80R, SAMS – A80S, SFDW – D64A, CHUMS – F17, FHA Connection – F17C, SFDMS – F42D, ARRTS – F51A, CAIVRS – F57, Title I Insurance and Claims – F72, FHASL – P013, NTHHQ – P16 (the Lender List functionality on the HUD.GOV portal)
	Others? (specify):
	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)?

	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:

Y	System users must log-in with a password (Please specify password type) External Users connect through FHA Connection and use those credentials. Internal Users use Single Sign On and use their H and C-ID credentials. Both internal and external users follow HUD policies through re-use of existing system protocols.
Y	When an employee leaves: <ul style="list-style-type: none"> How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? As soon as network credentials are revoked (typically, through the HUDGONE process). How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve):

	User ID's are in the Oracle/Siebel Federal Financial Services Platform (FFSP) are typically preserved in the user tables for historic continuity and record, but access privileges are revoked when HUD network credentials are removed
Y	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system: Less than 10 (Currently 4 Siebel Business Administrators, 4 Business Managers/Directors) Limited/restricted access rights to only select data: All Users (More than 15,000 including staff of approved external users). All users have access to a portion of the system and corresponding data. Security steps like obscuring full SSN's, compartmentalizing data, etc., reduce the risk of inappropriate user access.
N/A	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):
Y	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: HUD's systems operate in a federated computing environment, and each system conforms to HUD's overall security, privacy and data protection practices. Compliance with these practices are documented in the CSAM system, and regularly monitored.
Y	Other methods of protecting privacy (specify): Some LEAP users (those applying for approval as FHA Lenders) receive limited duration credentials which are used ONLY during the application period, and which automatically expire after a decision is rendered. Credentials have several automated expiration thresholds, based on periods of inactivity, application status and overall period since issuance.
	Comment:
<p>Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated.</p> <p>Privacy risks are currently identified and documented through the CSAM compliance process. Additionally, LEAP is built on the Oracle/Siebel FFSP and as such is subject to that platform's security structure. Lastly, the Oracle/Siebel FFSP is maintained by the HUD HITS contractor, who enforces HUD's security requirements (which in turn mitigates privacy risk).</p>	

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

Mark any that apply

X	Name:
X	Social Security Number (SSN)

	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
X	Other (specify):
	None
	Comment:

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?**

The initial SORN for LEAP was published prior to its initial roll-out in May 2012. Additionally, information about HUD's privacy policy is available on the lo-in page for applicants. Users of LEAP 3.0 will leverage the notices provided on FHA Connection.

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

No. Information is required to make business decisions.

- 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, specific consent for particular uses of data is not sought. All information collected is required in order for HUD to comply with regulation and policy.

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?

Information is retained in conformity with HUD policies. The need for specific modifications to the HUD data retention policy for LEAP will be considered on a case-by-case basis.

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

No

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

LEAP data retention policies are established balancing the information needs of the agency with the privacy rights of individuals. Because the nature of mortgage fraud can often take years to uncover, the personal information of key principals must be retained until the likelihood of negative impacts to FHA's Mutual Mortgage Insurance Fund (MMI Fund) from approval of "bad actors" burns off over time. At this stage, the length of retention strikes an appropriate balance with the risk of loss to the fund and the ability to attempt to recover losses from bad actors. PII is not retained as a matter of course but in order to protect the integrity of the Fund.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Privacy Office examined the LEAP 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 requirements are addressed. A SORN is required for this system and has been submitted to the Privacy Office of Approval. The Program Office is required to re-certify the IPA NLT February 20, 2016, in compliance with the FISMA requirements. Approval of this assessment is recommended.

