

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

Office of the Chief Financial Officer

Line of Credit Control System (LOCCS)

Privacy Impact Assessment
Version 3.2013

June 5, 2013

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.

/s/ Christopher B. Davies

Christopher B. Davies

Deputy Assistant Chief Financial Officer for Systems
Office of the Chief Financial Officer
U.S. Department of Housing and Urban Development

6/19/2013

Date

/s/ Christopher B. Davies for

Nita Nigam

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

6/19/2013

Date

/s/ Simin D. Narins

Simin D. Narins

Director, Financial Systems Quality Assurance Division
Office of the Chief Financial Officer

6/19/2013

Date

/s/ Donna Robinson-Staton

Donna Robinson-Staton

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

6/18/2013

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 2: Type of electronic system or information collection.....	9
Question 3: Explain by Line of Business why the personally identifiable information is 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 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 technical 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 be obtained from HUD’s 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:
LINE OF CREDIT CONTROL SYSTEM (LOCCS)**

**(for IT Systems: 025-00-01-01-01-1010-00-402-126
and PCAS #202540)**

June 5, 2013

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) (<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 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 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

Subject matter expert in the program area: Christopher B. Davies, Director, Financial Systems Maintenance Division, Office of the Chief Financial Officer, (202) 402-3758

Program Area Manager: Nita Nigam, Acting Assistant Chief Financial Officer for Systems, Office of the Chief Financial Officer, (202) 402-6850

IT Project Leader: Michael A. Pinckney, Office of Systems Integration & Efficiency, Office of the Chief Information Officer, (202) 402-4876

For IT Systems:

- **Name of system:** Line of Credit Control System (LOCCS)
- **PCAS #:** 202540
- **OMB Unique Project Identifier #:** 025-00-01-01-01-1010-00-402-126
- **System Code:** A67
- **Development Date:** 11-1-1983
- **Expected Production Date:** N/A

For Information Collection Requests:

- **Name of Information Collection Request:** LOCCS Voice Response System Access Authorization (HUD-27054); Direct Deposit Sign-Up Form (SF-1199A)
- **OMB Control #:** 2535-0102; 1510-0007

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?** Information collected includes name, social security number, address, bank routing number, and deposit account number.
- From whom is the information collected (i.e., government employees, contractors, or consultants)?** Information is collected from grant recipients.
- What is the functionality of the system and the purpose that the records and/or system serve?** The purpose of the system is to process and make grant, loan, and subsidy disbursements. LOCCS ensures that payments are made in a timely manner thus achieving efficient cash management practices. Its function is to create accounting transactions with the appropriate accounting classification elements to correctly record disbursements and collections to the grant/project level subsidiary.

- d. **How is information transmitted to and from the system?** Information is transmitted through electronic automated interfaces.
- e. **What are the interconnections with other systems?**
- A21-NLS to A67-LOCCS** -- Interest and collection activity is sent to LOCCS in order for LOCCS to batch and prepare a PAS transaction to send to PAS.
- A67-LOCCS to A21-NLS** – LOCCS returns confirmation of any “R”quest file activity as well as any Section 8 Housing offset activity. Some Multifamily Housing properties receiving Section 8 subsidy, also have a Section 202 loan against the property. Rather than the owner paying the loan separately back to HUD, their Section 8 subsidy is “offset” by the amount owed on the loan for that month.
- A75I-PSCRS/NFC to A67-LOCCS** -- The National Finance Center (NFC) file contains records of all active HUD employees, and is used by HUDCAPS for personnel and payroll processing. LOCCS cross references active HUD users to the NFC file by employee SSN. If the active HUD user SSN is not found in the NFC file, their LOCCS UserID is immediately terminated, and an email of terminated users is sent to OCFO Security staff.
- A67-LOCCS to A75R-Data Mart** -- Key LOCCS data is extracted and provided to the Data Mart for OCFO analysis and report/extract generation.
- A96-PAS to A67-LOCCS** -- To provide the latest contract information and obligation balances to LOCCS, prior to the LOCCS overnight payment cycle. This information is used in the final payment and posting decision by LOCCS prior to releasing any payments to Treasury.
- A67-LOCCS to A96-PAS** - This interface provides account posting information to PAS. Most of the transactions are disbursement transactions; however LOCCS also sends PAS receivable/collection information and for some programs, recapture transactions.
- C04-IDIS to A67-LOCCS** – Grantees request payment in the IDIS application and if approved, batched and sent to LOCCS for payment.
- A67-LOCCS to C04-IDIS** – LOCCS returns confirmation of any “R”quest file activity as well as any Ft. Worth/LOCCS/PAS activity as noted below.
- C08A-DRGR to A67-LOCCS** – Grantees request payment in the DRGR application and if approved, batched and sent to LOCCS for payment.
- A67-LOCCS to C04-IDIS** -- LOCCS returns confirmation of any “R”quest file activity as well as any Ft. Worth/LOCCS/PAS activity as noted below.
- D08-BOND/MAPPER to A67-LOCCS** – Years ago Public Housing Authorities (PHAs) raised capital by issuing BONDS. The amortized BOND repayment schedule is held in D08 and generally every six months a payment is made to the Fiscal Agent managing the security. The Fiscal Agent is then responsible for paying the individual BOND holders.
- A67-LOCCS to D08-BOND/MAPPER** – LOCCS returns confirmation of any “R”quest file activity.
- A67-LOCCS to DRC Contractor** – LOCCS generates numerous letters to grantees informing them of late documents that are due, or security letters notifying them of their UserID/Password or to Approving Officials informing them

recertification of their staff is due.

F87-TRACS to A67-LOCCS -- To provide Section 8 Multifamily Housing payment request to LOCCS.

A67-LOCCS to F87-TRACS -- To provide confirmation of “R”request file payment activity back to TRACS. In addition OCFO Ft. Worth activity on Section 8 Housing contracts are sent back, including (but not limited to) Manual Payments, Treasury Rejection information and receivable/collection activity.

A67-LOCCS to Microsoft Outlook – Numerous types of emails are sent to both HUD Staff and outside Business Partners. Business Partners receive payment confirmation emails and portfolio change emails. HUD staff receives reports, and some program offices receive attached files containing various extract information relevant to their program.

A67-LOCCS to P033-EIS (Executive Information System) – This is an extract of PIH Budget Line Item programs, containing Vendor and project level information.

A67-LOCCS to Treasury – Vouchers selected for payment are batched into Treasury schedule(s) and sent to the IBM for transmission to Treasury. EFT payments are batched separately from Check payments.

Pay.gov to A67-LOCCS – Information on financial collections received by Pay.gov on behalf of Housing and Urban Development are retrieved and stored for further transmission.

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)?

- Executive Order 9397, “Numbering System for Federal Accounts Relating to Individual Persons,” 1943.
- Executive Order 13478, “Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers,” 2008.
- The Housing and Community Development Act of 1987, 42 U.S.C.3543
- Sec. 113 of the Budget and Accounting Act of 1951 (31 U.S.C.66a)
- The Chief Financial Officers Act of 1990 (31 U.S.C. Sec. 501, et. Seq.)

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 type="checkbox"/>	<input checked="" 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"/>

B. If this is an existing electronic system has the system undergone any changes (since April 17, 2003)? If an existing system, when was the system developed? 11/1/1983	Yes <input type="checkbox"/>	No <input checked="" 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:		

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 <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 is 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): Disbursement of funds to subsidy recipients
	Comment: Information is used to identify the correct recipients due payments and to direct payments to the correct bank accounts.

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 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?
	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):
	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 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

	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): [Individuals may opt-out to provide personal information only where the application is using SSN for identity management.](#)

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technical 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)? HUD terminates the User ID when advised by the user's Approving Official during the quarterly user recertification process, when advised of a user's change of duties, or systematically when the user leaves the Department. How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): When the User ID record is removed, the employee no longer has access to LOCCS.
✓	<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: 5 users. Limited/restricted access rights to only selected data: 23459 users.
✓	<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): Infrastructure contractors managed by OCIO are responsible for system storage media. Individual users agree to comply with the Department's Information Technology Security Policy Handbook when applying for LOCCS access.</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: The security administrator is responsible for implementing controls over sensitive personal information. Access to sensitive information is controlled through a User ID and password. Access profiling restricts access to users with a business need-to-know.</p>
	Other methods of protecting privacy (specify):
	Comment:
<p>Privacy Impact Analysis: The OCFO has identified privacy risks associated with the type of information collected for accessing LOCCS. The main concern is the collection of SSN (Social Security Number) to verify the identities of users. The risk of collecting SSN is that it can be misused or disclosed for an unauthorized purpose. OCFO has taken steps forward in its efforts to evaluate its holdings of PII and to eliminate unnecessary collections. Only information about individuals that is relevant and necessary to</p>	

accomplish HUD’s mission is maintained. The data maintained in LOCCS has the appropriate administrative, technical, and physical safeguards to protect the information. SSN is no longer required on the HUD LOCCS access form (for internal users).

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): User ID
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	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? Yes. The following privacy policy is included on the LOCCS Voice Response System Access Authorization Form (HUD-27054):**

Public reporting burden for this collection of information is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. This agency may not collect this information, and you are not required to complete this form, unless it displays a currently valid OMB control number.

HUD implemented the Line of Credit Control System/Voice Response System (LOCCS/VRS) to process requests for payments to grantees. Grant recipients fill out a voucher form for the applicable HUD program with all the necessary information prior to making a telephone call using a touch tone telephone to initiate the drawdown process. The grantee will be prompted for entering the information and for confirming information that is spoken back by the VRS simulated voice. This information is required to obtain benefits under the U.S. Housing Act of 1937, as amended. The information requested does not lend itself to confidentiality.

Privacy Act Statement: Public Law 97-255, Financial Integrity Act, 31 U.S.C. 3512, authorizes the Department of Housing and Urban Development (HUD) to collect all the information which will be used by HUD to protect disbursement data from fraudulent actions. The Housing and Community Development Act of 1987, 42 U.S.C.3543 authorizes HUD to collect the SSN. The purpose of the data is to safeguard the Line of Credit Control System (LOCCS) from unauthorized access. The data are used to ensure that individuals who no longer require access to LOCCS have their access capability promptly deleted. Provision of the SSN is mandatory. HUD uses it as a unique identifier for safeguarding the LOCCS from unauthorized access. This information will not be otherwise disclosed or released outside of HUD, except as permitted or required by law. Failure to provide the information requested on the form may delay the processing of your approval for access to LOCCS.

- b. Do individuals have an opportunity and/or right to decline to provide information?** Yes. Individuals may opt-out to provide personal information only where the application is using SSN for identity management.

- 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 be obtained from HUD's 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?** The electronic records are maintained for 7 years and destroyed in accordance with schedule 20 of the National Archives and Records Administration General Records Schedule as specified in HUD Handbook 2225.6 Records Disposition Schedule Appendix 14, HUD Handbook 2228.1 Records Disposition Schedule Management Chapter 9, and HUD Handbook 2228.2 General

Records. Other materials, including hard copy printouts derived from electronic records created on an ad hoc basis for reference purposes or to meet day-to-day business needs, are destroyed when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

- 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 LOCCS include the possibility of data being accessed by unauthorized personnel and compromised PII (Personally Identifiable Information). Risks to the data in LOCCS are mitigated through the use of system scans, testing, and reviews.**

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Line of Credit Control System (LOCCS) 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 LOCCS is required by the Privacy Office no later than June 20, 2015.