U.S. Department of Housing and Urban Development

Office of Housing

Debt Collection and Asset Management System
Privacy Impact Assessment
Version 3.2013

April 24, 2014

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Debt Collection and Asset Management System – Title I Notes and Generic Debts**. 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.

__X__   **The document is accepted.**

_____   **The document is accepted pending the changes noted.**

_____   **The document is not accepted.**

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

SYSTEM OWNER   6/12/14
Date
Kathleen S. Malone
Office of Financial Services, Director
U. S. Department of Housing and Urban Development
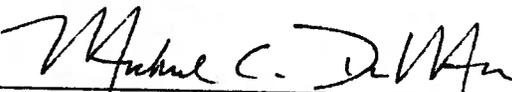
PROGRAM AREA MANAGER   4/25/14
Date
Michael C. DeMarco
Financial Operations Center, Director
U. S. Department of Housing and Urban Development
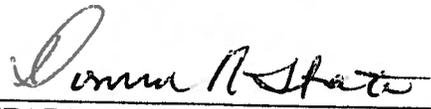
DEPARTMENTAL PRIVACY ACT OFFICER   7/1/14
Date
Donna Robinson-Staton
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

TABLE OF CONTENTS

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
DEBT COLLECTION AND ASSET MANAGEMENT SYSTEM

OMB Unique Identifier: 025-00-01-01-02-1080-00-307-116
and PCAS # 00251310

February 4, 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 Handbook1325.1 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 (Office of Finance and Budget)
Subject Matter Expert in the Program Area: John C. Mentes
Program Area Manager: Michael C. DeMarco
IT Project Leader: Hassan B. Zeraat

For IT Systems:
- **Name of system: Debt Collection and Asset Management System**
- **PCAS #: 00251310**
- **OMB Unique Project Identifier #: 025-00-01-01-02-1080-00-307-116**
- **System Code: F71/F71A**
- **Development Date: N/A – system deployed in 1983**
- **Expected Production Date: N/A – lifecycle stage is steady state**

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

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

a. **What is the personal information being collected?** Name, address, income/financial data, employment history, Social Security Number, Tax Identification Number, Employee Identification Number, FHA Case Number, date of birth, telephone number, and bank account.

b. **From whom is the information collected (i.e., government employees, contractors, or consultants)?** Information is collected from government employees, contractors, and the public (debtor-customers).

c. **What is the functionality of the system and the purpose that the records and/or system serve?** The system is used for collecting and servicing consumer and commercial debts owed to the Federal Housing Administration. The records contain information pertaining to debts and to indebted individuals.

d. How information is transmitted to and from the system? Information is transmitted to the system both electronically (via batch processing) and manually (online through a screen). Information is transmitted from the system electronically (via batch processing).

e. What are the interconnections with other systems? The system interconnects with the Title I Insurance and Claims System (HUD), Credit Authorization Interactive Verification System (HUD), FHA Subsidiary Ledger (HUD), Do Not Pay Portal (Treasury), Treasury Offset Program (Treasury), FedDebt (Treasury), Pay.gov (Treasury and Federal Reserve Bank of Cleveland), Bank of America Lockbox (Treasury), U.S. Bank (Treasury), Equifax (credit bureau), Experian (credit bureau), TransUnion (credit bureau), Innovis (credit bureau), Dunn and Bradstreet (credit bureau).

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)? 42 U.S.C 3543 (The Housing and Community Development Act of 1987), OMB Circular A-129: Policies for Federal Credit Programs and Non-Tax Receivables, 24 CFR §201.6, 24 CFR §17.76, 31 CFR §285, 31 CFR §901, §6050 P(a) of U.S. Tax Code, Improper Payments Elimination and Recovery Improvement Act of 2012 (31 U.S.C. 3321, Pub. Law No. 112-248, 126 Stat. 2390 (2013)), and OMB Memorandum M-12-11: Reducing Improper Payments through the "Do Not Pay List".

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)?	☐	☒
Does the system require authentication?	☒	☐
Is the system browser-based?	☒	☐
Is the system external-facing (with external users that require authentication)?	☐	☒

	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? 1983	☒	☐
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?	☒	☐

If yes, please explain: To implement the requirements set forth in the Improper Payments Elimination and Recovery Improvement Act of 2012 (31 U.S.C. 3321) the system sends a file containing the names and tax identification numbers of delinquent debtors to HUD's CAIVRS system which is subsequently sent to Treasury's Do Not Pay Portal for the purpose of eliminating and preventing improper payments.		

	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
X	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:

X	Credit checks (eligibility for loans) Credit Authorization Interactive Verification System (CAIVRS/F57)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
X	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	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): Debt Collection

X	Treasury Offset Program: administrative offset of federal and state payments and federal salaries and pensions
X	Treasury Cross Servicing Program: private collection agencies and administrative wage garnishment
X	Credit Bureau Reporting
X	Report Discharge of Indebtedness to IRS (1099-C)
X	Report Mortgage Interest Paid to IRS (1098)
X	Do Not Pay (Treasury): eliminate improper payments

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:

X	Federal agencies? Department of the Treasury, Internal Revenue Service, and Department of Justice
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	FHA-approved lenders?
X	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
X	HUD module/application? (specify the module(s)/application(s) name) Credit Authorization Interactive Verification System (CAIVRS/F57)
X	Others? (specify): Private collection agencies contracted by the Department of the Treasury

	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: Personal information is required for participating in federal credit programs.

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: alphanumeric type.
X	When an employee leaves: • How soon is the user ID terminated? Between 1 day and 1 week. • How do you know that the former employee no longer has access to your system? The system reflects that his or her access credentials have been revoked.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system: 40 • Limited/restricted access rights to only selected data: 4
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? Yes. Secured in locked cabinets. There are plans in place to secure them in a separate locked room.
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? The receiving system or organization is responsible for protecting the privacy of the information received by DCAMS. The system that receives information from DCAMS is subject to the same laws regulating privacy protections that pertain to DCAMS.

X	Other methods of protecting privacy (specify): System users are subject to a background check prior to being granted system access. System users are required to take privacy training.
	Comment:

Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated. Main risk is improper use of data by personnel with authorized access to the data. A privacy risk is the improper use of sensitive information by personnel who have authorized access to the system and the records stored on the system. This risk is mitigated by the agency requirement that system users undergo a background check before being granted access; by training users in the proper handling of sensitive information (annually); by having users sign rules of behavior that state the "does and don'ts" when using the system and accessing its data. Another risk is the access by unauthorized users, which is mitigated by the implementation of effective security controls as prescribed by Federal Information Security Management Act of 2002, in National Institute of Standards, Special Publications 800-53, Rev. 4 and 800-122, and in Federal Information Processing Standards Publications 199 and 200.

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): **Account number**
	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 Systems of Records Notice was published in the Federal Register on November 13, 2007 (and corrected December 10, 2007) in Volume 72, Number 218 [Docket No. FR-5130-N-14]. This document is available at http://www.gpo.gov/fdsys/pkg/FR-2007-11-13/pdf/E7-22077.pdf and http://portal.hud.gov/hudportal/documents/huddoc?id=DOC_15193.pdf.

b. **Do individuals have an opportunity and/or right to decline to provide information?** No. Providing this information is required to participate in the FHA programs as a lender, borrower, or other participant.

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. The collected information is required for participation in FHA programs.

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?**

The information is permanently retained digitally in back-up media. This is consistent with HUD's Records Disposition Schedules 13 and 21. The information is retained permanently, in part, to comply with 31 U.S.C. §285.13 (barring delinquent debtors from obtaining federal loans or loan insurance or guarantees); and, in part, to assist the public and the debtor customers by keeping case information available in the event the debt shows up in public records and in the federal government's Do Not Pay list.

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

Yes. (See Handbook 2225.6 REV-1, Appendix 21, CHG-68, pages 1-8, dated 1/07 and Appendix 13, pages 1-12.)

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

There is no risk with the permanent electronic retention of data, which includes personal information. The data for retired accounts are stored on back-up media that is not accessible by the system users or through a network connection. The backed-up data may be made available only by reactivating the account record. The access to the functionality for reactivating a case is limited to select personnel; and when a case is reactivated, a record of the transaction is reported to management.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Privacy Office examined the Debt Collection and Asset Management System (DCAMS) 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 PII. This was a response to the update/recertification of the IPA and since no changes have occurred to the system of the collection the SORN is not required to be updated at this time. The Program Office will re-certify the IPA NLT March 24, 2016, in compliance with the FISMA requirements. Approval of this assessment is recommended.