U.S. Department of Housing and Urban Development

Office of General Counsel
Office of Fair Housing and Equal Opportunity
Office of Lead Hazard Control and Healthy Homes
Office of Departmental Operations and Coordination

HUD Enforcement Management System (HEMS)

Privacy Impact Assessment
Version 3.2013

June 3, 2014

Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for **the HUD Enforcement Management System (HEMS)**. 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.

Patrina Munson
Office of Fair Housing and Equal Opportunity

9/29/2014
Date

Nina Aten
Office of General Counsel

9-29-14
Date

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

9-29-14
Date

Table of Contents

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. 10
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 **16**

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
HUD ENFORCEMENT MANAGEMENT SYSTEM (HEMS)

(for IT Systems: [Insert OMB Unique Identifier]
and PCAS# 561500)

June 3, 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: Regulatory, Legislative and Enforcement Segment
Subject Matter Expert in the Program Area: Nina Aten
Program Area Manager: Patrina Munson
IT Project Leader: Nina Aten

For IT Systems:

- **Name of system:** HUD Enforcement Management System (HEMS)
- **PCAS #:** 561500
- **OMB Unique Project Identifier #:**
- **System Code:** V05
- **Development Date:**
- **Expected Production Date:** October 15, 2014

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?** (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)

HEMS will collect names, addresses, gender/sex, birth dates, company names, phone numbers, ethnicity, race, religion, investigative case names, party/witness names

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

Information may come from HUD Field Office staff, HUD partners/grantees, state and local government agencies, and private sector, including doctors by Paper and CDs by Mail and/or couriers; FAX, and/or email.

This information is not entered by the public in HEMS. We expect HEMS to have PII information through case referrals sent by various program offices and the Office of Inspector General.

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

The HUD Enforcement Management System (HEMS) project will provide resources needed to develop software modules to integrate disparate enforcement systems and applications with varied functionality (such as Enforcement Center Information System (ECIS), Departmental Enforcement Center Management System (DECMS), Enforcement Center Program Compliance Integration System (ECPCIS), Microsoft SharePoint) and program office HUD business systems (such as the iREMS, Title Eight Automated Paperless On-line Tracking System (TEAPOTS), Lead Enforcement Tracking System (LETS), Public Housing Section 8 investigative system, and any system purposed to support Davis-Bacon Act to include LR 2000) to gain operational efficiency by reducing redundant data entry and automating manual processes across all HUD enforcement systems.

The HEMS project will serve over 9,000 internal and external users who use several internal disparate systems and applications on a daily basis for providing enforcement services to all HUD program offices. The project will provide cross-organizational reporting and data sharing ability in relation to the various systems and applications, which currently is a cumbersome process thus supporting the objective of reducing obsolescence, redundancy and increasing compatibility across systems.

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

Federal government employees will enter information into the system and data output will be available for review by internal and external users. Input will be entered via intranet application. Information that is on paper is scanned – if electronic files are sufficiently compatible, information is transferred; otherwise manual entry.

e **What are the interconnections with other systems.**

The HUD Enforcement Management System (HEMS) project will provide resources needed to develop software modules to integrate disparate enforcement systems and applications with varied functionality (such as Enforcement Center Information System (ECIS), Departmental Enforcement Center Management System (DECMS), Enforcement Center Program Compliance Integration System (ECPCIS), Microsoft SharePoint) and program office HUD business systems (such as the iREMS, Title Eight Automated Paperless On-line Tracking System (TEAPOTS), Lead Enforcement Tracking System (LETS), Public Housing Section 8 investigative system, and any system purposed to support Davis-Bacon Act to include LR 2000) to gain operational efficiency by reducing redundant data entry

and automating manual processes across all HUD enforcement systems. HEMS will extract and/or link to HUD program databases (iREMS, PIC, IDIS, GPM, LOCCS).

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 Deputy Secretary has directed the Regulatory, Legislative, and Enforcement IT Investment Segment to consolidate all HUD Enforcement systems into one. This consolidation will combine existing systems from OGC, OHHLHC, FHEO and ODOC to include the following systems: ECIS, DECMS, ECPCIS, TEAPOTS, LETS, and LR 2000. Below is a list of the legal authorities for HEMS to collect PII:

- Title VIII of the Civil Rights Act of 1968, as amended by the Fair Housing Act of 1988 (42 U.S.C. 3601 et seq.),
- Title VI of the Civil Rights Act of 1964 (42 U.S.C. Sections 2000d-2000d-7),
- Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 791 et seq.),
- Section 109 of Title I of the Housing and Community Development Act of 1974 (42 U.S.C. 5301-5321),
- Title II of the American Disabilities Act of 1990 (42 U.S.C. 12101 et seq.),
- Age Discrimination Act of 1975 (42 U.S.C. Sections 6101-107),
- Title IX of the Education Amendments Act of 1972 (Title 20 U.S.C. Sections 1681-1688), and
- Architectural Barriers Act of 1968 (42 U.S.C. 4151 et seq.).
- Title 2, CFR, Parts 180 and 2424 authorize HUD to impose the administrative sanctions of suspensions and debarments. Title 2 CFR Part 2424, Subpart J authorizes HUD to impose the administrative sanctions of limited denials of participation.
- Lead Disclosure Rule, that applies to target housing, statutorily defined as housing built before 1978 with exemptions and exceptions
- Lead Safe Housing Rule that applies to target housing that receives federal assistance.

Information will be on leases, disclosure forms, inspection reports, referral forms, and may include names, addresses, ages (occasionally the landlord records SSN, so it may be in a digital file- SSN will not be recorded in the HEMS data system and will be struck out or blackened before scanning); health department reports may include blood lead levels.

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? _____	☐	☐
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:		

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):	
	Conversion: When paper-based records that contain personal information are converted to an electronic system
	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
	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)
X	**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)
	New Public Access: When new 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)

	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)
	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

D. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.	
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 new or automated)
	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:

X	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:

X	Federal agencies?
	State, local, or tribal governments?
X	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 for not for sharing with other government agencies)?

X	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): Users are not required to enter personal information.

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): WASS Authentication, and username/password authentication
	When an employee leaves: • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? Immediately upon notification. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): System access is manually removed.
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: Limited/restricted access rights to only selected data:
	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):
	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:
	Other methods of protecting privacy (specify):
	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

X	Name:
	Social Security Number (SSN)
	Identification number (specify type):
X	Birth date
X	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
X	Home telephone
X	Personal e-mail address
X	Other (specify): gender/sex, company names, religion, investigative case names, party/witness names
	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? SORN to be published**

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

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?**

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 retention period for the information in HEMs is maintained for the life of the case to support the activity and other enforcement activities that may become related to the case. When the life of the case is closed (the case is no longer needed for administrative or reference use, or to satisfy preservation requirements), and a final determination has been made of the case records, records in the system are maintained in accordance with the approved records schedule, HUD's Records and Disposition Schedule Handbook 2225.6, Appendix 50.1 Historic or significant investigation files are PERMANENT, pending appraisal by NARA. Files Transfers are made to the National Archives and Records Administration every 5 years, when applicable (Including a listing of restricted data fields, which remain in place 30 years after which a final appraisal is conducted.

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

<<ADD ANSWER HERE>>

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

<<ADD ANSWER HERE>>

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER