

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

Office of Inspector General

**Distributed Computing Environment
(DCE)**

Privacy Impact Assessment

September 21, 2010

Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for **IG's DCE , which also includes the following applications AutoAudit, Hotline Tracking System, Auto Investigation / Case Management Information Subsystem, and Employee Database Subsystem**. 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

By providing your signature below you agree/endorse the information that has been provided for respective area/application is current and accurate

/s/ Karen Cookson

10/08/2010

PROGRAM AREA MANAGER

Date

Karen Cookson (AutoAudit)
Office of Audit

/s/ Michael R. Kirby

10/21/2010

PROGRAM AREA MANAGER

Date

Michael Kirby (Hotline Tracking System)
Office of Management

/s/ Melanie Bryant

09/30/2010

PROGRAM AREA MANAGER

Date

Melanie Bryant (CMISS/IA)

[/s/ Derek Fitzgerald](#)

10/20/2010

PROGRAM AREA MANAGER

Date

Derek Fitzgerald (EDSS)

[/s/ James Szymanski](#)

10/22/2010

SYSTEM OWNER

Date

James Szymanski
OCIO, HUD OIG

[/s/ Donna Robinson-Staton](#)

11/15/2010

CHIEF PRIVACY OFFICER

Date

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

Table of Contents

SECTION 1: BACKGROUND.....	5
SECTION 2 - COMPLETING A PRIVACY IMPACT ASSESSMENT	8
Section 2.1 - AutoAudit PIA.....	8
Section 2.2 - Hotline Tracking System PIA.....	17
Section 2.3 - Auto Investigation / Case Management Information Subsystem PIA.....	25
Section 2.4 - Employee Database Subsystem PIA.....	36
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	44

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
DISTRIBUTED COMPUTER ENVIRONMENT (DCE) AND ITS SUBSYSTEMS**

DCE OMB Unique Identifier: 025-00-02-00-01-1999-00

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 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

Section 2.1 - AutoAudit PIA - **FINAL**

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 Audit

Subject matter expert in the program area: Karen Cookson, Office of Inspector General, Technical Oversight and Planning

Program Area Manager: Karen Cookson, Office of Inspector General, Technical Oversight and Planning

IT Project Leader: Marcieta Thompson, Office of Inspector General, Information Systems Division

For IT Systems:

- **Name of system:** AutoAudit
- **OMB Unique Project Identifier #:** N/A
- **System Code:** N/A

For Information Collection Requests: N/A. Not an ICR AutoAudit is an existing system

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

Question 1: Provide a brief description of what personal information is collected: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

Personally identifiable information collected in the course of conducting an audit is used to obtain and to afford a reasonable basis for the auditor's opinions and conclusions to meet the required audit objective, i.e., to determine program eligibility. Personally identifiable information is collected on a case-by-case basis, as needed, to meet the required audit objective.

Auditors may collect personally identifiable information during the course of collecting audit evidence. Auditors' findings and conclusions must be supported by sufficient, competent, and relevant evidence. Audit evidence may be categorized as physical, testimonial, documentary, or analytical. The auditors obtain physical evidence by direct inspection or observation of activities of people, property, or events, such as memoranda summarizing the matters inspected or observed photographs, charts, or actual graphs. The auditors obtain testimonial evidence through statements received in response to inquiries or through interviews. The auditors obtain documentary evidence, including letters, contracts, accounting records, invoices, cancelled checks, electronic documents such as electronic email, etc. The auditors obtain analytical

evidence through computations, comparisons, separation of information into components, and rational arguments.

Personally identifiable information may also be collected by ad hoc queries of HUD's automated systems such as the Integrated Real Estate Management System (iREMS), the PIH Inventory Management System formerly Information Center (PIC), the Single Family Enterprise Data Warehouse, the Tenant Rental Assistance Certification System (TRACS), etc. In addition, personally identifiable information may be collected by ad hoc queries of commercial sources such as ChoicePoint and LexisNexus.

System Description

The U. S. Department of Housing and Urban Development (HUD) Inspector General is one of the original 12 Inspectors General authorized under the Inspector General Act of 1978. The Office of Inspector General (OIG) is an independent and objective organization responsible for audits and investigations relating to program and operations of the Department.

The Office of Audit is an organizational unit within HUD OIG, which is responsible for the development and implementation of the Department's audit activities. This includes:

- A. Conducting and supervising independent and objective audits of agency programs and operations. This includes the authority to determine what audits to perform and to access all information necessary to complete the audits.
- B. Promoting economy, effectiveness, and efficiency within the agency.
- C. Preventing and detecting fraud, waste, and abuse in agency programs and operations.
- D. Reviewing and making recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- E. Keeping the agency head and the Congress fully and currently informed of problems in agency programs and operations.

The Office of Audit is led by the Assistant Inspector General for Audit (AIGA). The Office of Audit has a Headquarters Office organized into three divisions in Washington D.C., eight Regional Offices, with Field Offices located within Regions, and an office for Hurricane Recovery. The Office of Audit employs approximately 300 staff.

AutoAudit for Lotus Notes

The Office of Audit (OA) uses a customized version of Paisley Consulting's AutoAudit for Lotus Notes application for managing its audit operations in a "paperless" work environment. The AutoAudit application allows users to create and store all of their audit documentation, such as audit programs, work papers, findings, memos, and audit reports in a Lotus Notes database where they can be easily retrieved for future use. It is important to note that AutoAudit is not a

database used for retrieving privacy information. Currently, there are about 300 AutoAudit users.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Social Security Number (SSN) Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs): The purpose of collecting SSNs is to make determinations if subjects are receiving HUD funding assistance. The authority is the Inspector General Act of 1978, 5 U.S.C. App.
<input checked="" type="checkbox"/>	Other identification number (specify type):
<input checked="" type="checkbox"/>	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
<input checked="" type="checkbox"/>	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
	Comment:

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
<input checked="" type="checkbox"/>	Gender/ sex
<input checked="" type="checkbox"/>	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Data collected includes salary, W-2s, bank account numbers, federal tax forms, federal/state assistance, alimony payments, etc.
<input checked="" type="checkbox"/>	Employment history:
<input checked="" type="checkbox"/>	Education level
	Medical history/ information
	Disability
	Criminal record
	Other (specify):
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)? All HUD OIG laptops have FIPS 140-2 approved hard drive encryption implemented.		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? HUD OIG information for AutoAudit is able to be accessed remotely via an encrypted VPN. Is remote access, VPN, telework optional and/or permitted? If permitted, specify remote access types.		
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department? Yes, the policy for utilizing remotes access is explained within the HUD OIG Rules of Behavior.		
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Yes, the policy that explains the how data is to stored/downloaded is explained within the HUD OIG Rules of Behavior.		
Comment:		

Question 3: Type of electronic system or information collection.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes	No
If yes, please proceed to answering the following questions.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Does the system require authentication?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input type="checkbox"/>

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? April 2006	Yes	No
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. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (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 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.

	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 4: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

<input checked="" type="checkbox"/>	Credit checks (eligibility for loans)
<input checked="" type="checkbox"/>	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
<input checked="" type="checkbox"/>	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
<input checked="" type="checkbox"/>	Loan default tracking
<input checked="" type="checkbox"/>	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

<input checked="" type="checkbox"/>	Eligibility for rental assistance or other HUD program benefits
<input checked="" type="checkbox"/>	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
<input checked="" type="checkbox"/>	Property inspections
	Other (specify):
	Comment:

Grants:

<input checked="" type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input checked="" type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

<input checked="" type="checkbox"/>	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

<input checked="" type="checkbox"/>	Employee payroll or personnel records
<input checked="" type="checkbox"/>	Payment for employee travel expenses
<input checked="" type="checkbox"/>	Payment for services or products (to contractors) – if any personal information on the payee is included
<input checked="" type="checkbox"/>	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 5: Will you share the information with others? (e.g., another agency for a programmatic purpose 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?
X	Others? (Specify): HUD officials, as needed for programmatic purposes. In addition, the information may be shared with the AUSA if there is a pending case.
	Comment:

Question 6: 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
X	No, they can’t “opt-out” – all personal information is required
	Comment:

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

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password
X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? Within 24 hours. • 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 an employee leaves the Department a MACD is completed the users laptop is confiscated and returned to HUD OIG WHQ, thus preventing VPN access, VPN, Email, AD and other accounts are deactivated.
X	<p>Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> • Full access rights to all data in the system: 40 <p>Limited/restricted access rights to only selected data: 300</p>
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): Yes Office access is by keycard, storage medium is secured when not in use according to the rules of behavior,</p> <p>Yes. Nightly incremental backup and weekly full backup. Stored in locked file cabinet in server room and accessible only by keycard from the standard office space.</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:</p>
X	Other methods of protecting privacy (specify):
	<p>Comment: AutoAudit is set up to limit the accessibility of the work papers to only the staff that need to have access. This can be limited even further, for example if the work involves Grand Jury testimony (6e).</p>

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): Records may be retrieved by computer search of the AutoAudit software, and/or by reference to a particular file number.
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes No (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

If yes, provide the Federal Register citation: [The system or records is entitled: OIG-5 AuditAudit of the Office of Inspector General. Please refer to this URL <http://www.hud.gov/offices/cio/privacy/sorninv.cfm> for the SORN in full text.](#)

Other Comments (or details on any Question above):

Section 2.2 - Hotline Tracking System PIA - FINAL

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: Program Integrity Division

Subject matter expert in the program area: Michael Kirby

Program Area Manager:

IT Project Leader: Dennis Raschka

For IT Systems:

- **Name of system:** HUD OIG Hotline Tracking System
- **OMB Unique Project Identifier #:** N/A
- **System Code:** N/A

For Information Collection Requests:

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

Question 1: Provide a brief description of what personal information is collected: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

The OIG Hotline database is based on an existing OIG database Case Management Information Subsystem (CMISS) developed by the Office of Inspector General. The database is a standalone system that is used exclusively by members of the OIG Hotline staff. Information in the database reflects information collected by Hotline staff on complaints made to the OIG. Database complaint information is analyzed by Hotline staff members to determine if the complaint is related to the OIG mission of waste, fraud, abuse, or serious mismanagement, in which case it will be addressed by OIG, or if it should be referred for address to another HUD office or other agency. Database information is used for Hotline cases that are referred internally to OIG's audit and investigative operations or externally to senior officials in the Department so that the substance of the complaint is addressed. Information in the Hotline database and in Hotline cases is in a Privacy Act system of records, and is therefore restricted.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Social Security Number (SSN) Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs): The purpose of collecting SSNs is to make determinations if subjects are receiving HUD funding

	assistance. The authority is the Inspector General Act of 1978, 5 U.S.C. App.
X	Other identification number (specify type):
X	Birth date
X	Home address
X	Home telephone
X	Personal e-mail address
X	Fingerprint/ other "biometric"
X	Other (specify): Relatives and Friends
	None
	Comment:

Personal/ Sensitive Information:

X	Race/ ethnicity
X	Gender/ sex
X	Marital status
X	Spouse name
X	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
X	Employment history:
X	Education level
X	Medical history/ information
X	Disability
X	Criminal record
	Other (specify):
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)? All HUD OIG laptops have FIPS 140-2 approved hard drive encryption implemented.		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? HUD OIG information for Hotline Tracking System is accessed remotely via an encrypted VPN/telework is permitted.		
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department? Yes, the policy for utilizing remotes access is explained within the HUD OIG Rules of Behavior.		

Is there a policy that identifies “if” or “if not” downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Yes, the policy that explains the how data is to stored/downloaded is explained within the HUD OIG Rules of Behavior.
Comment:

Question 3: Type of electronic system or information collection.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes	No
If yes, please proceed to answering the following questions.	<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 type="checkbox"/>	<input checked="" type="checkbox"/>

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? April 2006	Yes	No
	<input type="checkbox"/>	<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. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (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 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.

	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 4: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

<input type="checkbox"/>	Credit checks (eligibility for loans)
<input type="checkbox"/>	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
<input type="checkbox"/>	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
<input type="checkbox"/>	Loan default tracking
<input type="checkbox"/>	Issuing mortgage and loan insurance
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Rental Housing Assistance:

<input checked="" type="checkbox"/>	Eligibility for rental assistance or other HUD program benefits
<input checked="" type="checkbox"/>	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
<input checked="" type="checkbox"/>	Property inspections
<input checked="" type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Grants:

<input checked="" type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input checked="" type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Fair Housing:

<input checked="" type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Internal operations:

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

Other lines of business (specify uses):

Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?

Mark any that apply:

<input checked="" type="checkbox"/>	Federal agencies To relevant Federal agency charged with the responsibility for investigating or prosecuting such violation or enforcing or implementing such statute, rule or regulation. Refer to published SORN for additional details.
<input checked="" type="checkbox"/>	State, local, or tribal governments?
<input checked="" type="checkbox"/>	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
<input checked="" type="checkbox"/>	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
	Comment:

Question 6: 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
<input checked="" type="checkbox"/>	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): _ Anonymous, Confidential Compliance _____

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
X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? Within 24 hours. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): MACD is completed the users laptop is confiscated and returned to HUD OIG WHQ, thus preventing VPN access, VPN, Email, AD and other accounts are deactivated. HelpDesk request is submitted to IT requesting suspension of an employee's access to the system.
X	<p>Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> • Full access rights to all data in the system: 40 <p>Limited/restricted access rights to only selected data: 300</p>
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve):</p> <p>The OIG Hotline staff does not routinely use discs, tapes, or printouts. The OIG space in the Potomac Center Building where the Hotline computer system and the Hotline files are located is restricted to OIG personnel in that building. By OIG personnel, we mean full time OIG employees who work in the building and who have current security clearances. No one else has access. Everyone else is required to have an escort, including OIG personnel who work at the main HUD building, OIG contractors, HUD personnel, building maintenance, and construction workers. Cleaning staff is only allowed in the OIG area during normal working hours when OIG personnel are present. All manual files are located in file cabinets and file storage rooms that are lockable. Access to both storage areas are restricted to OIG personnel in the building.</p> <p>Hotline computer information never leaves the OIG area in the Potomac Center Building. Hotline files can leave the Potomac Center Building only if they are hand carried by Hotline staff and personally handed to OIG personnel located in restricted access areas of the HUD headquarters building. Hotline staff members are allowed to telework/utilize computers (laptops) outside the Department, but employees cannot carry Hotline computer information out of the Potomac Center Building.</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:</p>

	Other methods of protecting privacy (specify):
	Comment:

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

Mark any that apply

<input checked="" type="checkbox"/>	Name:
	Social Security Number (SSN)
<input checked="" type="checkbox"/>	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes No (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

If yes, provide the Federal Register citation: The system or records is entitled: [OIG-2:Hotline Compliant Files of the Office of Inspector General](#). Please refer to this URL <http://www.hud.gov/offices/cio/privacy/sorninv.cfm> for the SORN in full text.

Other Comments (or details on any Question above):

Section 2.3 – Auto Investigation (AI) Case Management Information Subsystem (CMISS) PIA - FINAL

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: HUD OIG Investigation

Subject matter expert in the program area:

Program Area Manager: Melanie Bryant 202.402.8166 mbryant@hudoig.gov

IT Project Leader: Philip Lord, plord@hudoig.gov

For IT Systems:

- **Name of system:** AI/CMISS
- **OMB Unique Project Identifier #:** N/A
- **System Code:**

For Information Collection Requests:

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

Question 1: Provide a brief description of what personal information is collected: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

The Housing and Urban Development (HUD) Office of Inspector General (OIG) Auto Investigation (AI) and Case Management Information System (CMISS) has been initiated to design, develop, produce, and deploy system that will fulfill the Office of Investigation's business and functional requirements. The System will replace the AI System that HUD OIG Investigations is currently using under Lotus Notes to manage their complaints, investigation cases and profiles. Until AI is fully phased out IG will continue to use both CMISS and AI data to fulfill functional requirements for IG investigations.

CMISS and AI will provide HUD OIG Investigations with a system to manage cases from their inception to closing via a centralized data repository of Case information. AI and CMISS and its environment will be a secure system where access to information is controlled via a formal process of checks and authorizations involving a hierarchical supervisory structure. Special Agents in Charge (SAC), Assistant Special Agents in Charge (ASAC), Supervisory Forensic Auditors (SFA), Forensic Auditors (FA), Special Agents (SA) and support staff document all steps in their assigned activities. Additionally, due to judicial involvement in some of the cases, the files kept and maintained by HUD OIG may be made available to the courts under Discovery.

AI and CMISS receive personnel information from HUDOIG's EDSS. CMISS does not transmit to any system at this time. Future requirements will include system integration with other HUD OIG applications such as Hotline and Audit.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Social Security Number (SSN) Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs): The purpose of collecting SSNs is to make determinations if subjects are receiving HUD funding assistance. The authority is the Inspector General Act of 1978, 5 U.S.C. App
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Other identification number (specify type): EIN OR TIN, • Drivers License (Issuing State and Country, Issue Date, Expiration/Renewal Date, License Number, Name on License) • Passport (Issue Date, Issuing Country, Passport Number, Expiration Date, Name of Passport, Place of Issuance) • Narcotics and Dangerous Drugs Information System Number (NADDIS) Federal Bureau of Investigation Number • State ID
<input checked="" type="checkbox"/>	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
<input checked="" type="checkbox"/>	Fingerprint/ other "biometric"
<input checked="" type="checkbox"/>	Other (specify): <ul style="list-style-type: none"> • Entity Name, • Place of Birth, • Alias, • Height, • Weight, • Hair and Eye Color, • Tattoos/Marks/Scars, • Contact Telephone Number, • Citizenship, • Emergency Contact (Phone Number, Address), and • Lead Information (Phone Number, Address)
	None
	Comment:

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
<input checked="" type="checkbox"/>	Gender/ sex
<input checked="" type="checkbox"/>	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
<input checked="" type="checkbox"/>	Employment history:
	Education level
	Medical history/ information
	Disability
<input checked="" type="checkbox"/>	Criminal record
<input checked="" type="checkbox"/>	Other (specify): <ul style="list-style-type: none"> • Spouse: Date of Birth, Address, Phone Number • Children: Date of Birth, Address, Phone Number • Father: Date of Birth, Address, Phone Number • Mother: Date of Birth, Address, Phone Number • Companion: Date of Birth, Address, Phone Number • Owner: Date of Birth, Address, Phone Number • President: Date of Birth, Address, Phone Number • Vice President: Date of Birth, Address, Phone Number • Secretary: Date of Birth, Address, Phone Number • Treasurer: Date of Birth, Address, Phone Number • Registered Agent: Date of Birth, Address, Phone Number • Incorporated/Date of Incorporation • Business Associations: Employer: Name, Address, Telephone Number Doing Business As (DBA): Name, Address, Telephone Number • Known Associates: Name, Address, Relationship, Also Known As, Date of Birth, SSN) • Group, Event, and Vehicle
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)? All HUD OIG laptops have FIPS 140-2 approved hard drive encryption implemented.		

What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? HUD OIG information for CMISS is able to be accessed remotely via an encrypted VPN. Is remote access permitted via VPN or telework permitted? Is specify types of telework permitted.
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department? Yes, the policy for utilizing remotes access is explained within the HUD OIG Rules of Behavior.
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Yes, the policy that explains the how data is to stored/downloaded is explained within the HUD OIG Rules of Behavior.
Comment:

Question 3: Type of electronic system or information collection.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes	No
If yes, please proceed to answering the following questions.	<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 type="checkbox"/>	<input checked="" type="checkbox"/>
Comment: System Deployed April 2010		

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? 2007 (implemented 2010)	Yes	No
	<input type="checkbox"/>	<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 checked="" type="checkbox"/>
If yes, please explain: Refer to section C. for explanation		

C. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

<input checked="" type="checkbox"/>	Conversion: When paper-based records that contain personal information are converted to an electronic system
-------------------------------------	---

X	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 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.

	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 4: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

<input type="checkbox"/>	Credit checks (eligibility for loans)
<input type="checkbox"/>	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
<input type="checkbox"/>	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
<input type="checkbox"/>	Loan default tracking
<input type="checkbox"/>	Issuing mortgage and loan insurance
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Rental Housing Assistance:

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

Grants:

<input type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Fair Housing:

<input type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Internal operations:

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

	Comment:
--	----------

Other lines of business (specify uses):

X	Investigations

Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)? Yes.

Mark any that apply:

X	Federal agencies?
X	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?
X	<p>Others: In addition to those disclosures generally permitted under subsection (b) of the Privacy Act of 1974, 5 U.S.C. 552a(b), records may also be disclosed routinely to other users under the following circumstances:</p> <ol style="list-style-type: none"> 1. In the event that records indicate a violation or potential violation of law, whether criminal, civil or regulatory in nature, the relevant records may be disclosed to the appropriate federal, State or local agency charged with the responsibility for investigating or prosecuting such violation or enforcing or implementing such statute, rule or regulation. 2. Records may be disclosed to a congressional office in response to an inquiry from that congressional office made at the request of the individual who is the subject of the records. 3. Records may be disclosed to HUD contractors, Public Housing Authorities or management agents of HUD-assisted housing projects, in order to assist such entities in taking action to recover money or property, where such recovery serves to promote the integrity of the programs or operations of HUD. 4. Records may be disclosed during the course of an administrative proceeding where HUD is a party to the litigation and the disclosure is relevant and reasonably necessary to adjudicate the matter. 5. Records may be disclosed to any source, either private or governmental, to

	<p>the extent necessary to elicit information relevant to an OIG investigation.</p> <p>6. Records may be disclosed to appropriate State boards of accountancy for possible administrative or disciplinary sanctions such as license revocation. These referrals will be made only after the independent auditor has been notified that the OIG is contemplating disclosure of its findings to an appropriate State board of accountancy, and the independent auditor has been provided with an opportunity to respond in writing to the OIG's findings.</p> <p>7. Records may be disclosed to DOJ for litigation purposes associated with the representation of OIG and/or HUD before the courts.</p>
	Comment:

Question 6: 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
X	No, they can’t “opt-out” – all personal information is required
	Comment:

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

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? Within 24 hours. • 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 an employee leaves the Department a MACD is completed the users laptop is confiscated and returned to HUD OIG WHQ, thus preventing VPN access, VPN, Email, AD and other accounts are deactivated.
X	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: 40 Limited/restricted access rights to only selected data: 300
X	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): Yes Office access is by keycard, storage medium is secured when not in use according to the rules of behavior, Yes. Nightly incremental backup and weekly full backup. Stored in locked file cabinet in server room and accessible only by keycard from the standard office space.
	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:

X	Other methods of protecting privacy (specify): Hard Drive encryption
X	Comment: Additionally, when Investigators are working from a remote location they remotely access CMISS through a VPN.

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)
X	Identification number (specify type): <ul style="list-style-type: none"> • EIN OR TIN, • Drivers License (Issuing State and Country, Issue Date, Expiration/Renewal Date, License Number, Name on License) • Passport (Issue Date, Issuing Country, Passport Number, Expiration Date, Name of Passport, Place of Issuance) • NADDIS • FBI Number • State ID
X	Birth date
X	Race/ ethnicity
X	Marital status
X	Spouse name (Date of Birth, Address, Phone Number)
X	Home address
X	Home telephone
X	Personal e-mail address
X	Other (specify): <ul style="list-style-type: none"> • Children: Date of Birth, Address, Phone Number • Father: Date of Birth, Address, Phone Number • Mother: Date of Birth, Address, Phone Number • Companion: Date of Birth, Address, Phone Number • Owner: Date of Birth, Address, Phone Number • President: Date of Birth, Address, Phone Number • Vice President: Date of Birth, Address, Phone Number • Secretary: Date of Birth, Address, Phone Number • Treasurer: Date of Birth, Address, Phone Number • Registered Agent: Date of Birth, Address, Phone Number • Incorporated/Date of Incorporation • Business Associations: Employer: Name, Address, Telephone Number Doing Business As (DBA): Name, Address, Telephone Number • Known Associates: Name, Address, Relationship, Also Known As, Date of Birth, SSN • Group, Event, and Vehicle • Criminal Record: Prior Arrest, Date History Checked, Scanned

	<p>Document/Photograph, Contact Agent</p> <ul style="list-style-type: none"> • Entity Name • Place of Birth • Alias • Height • Weight • Hair and Eye Color • Tattoos/Marks/Scars • Contact Telephone Number • Citizenship • Emergency Contact (Phone Number, Address) • Lead Information (Phone Number, Address)
	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes No (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

If yes, provide the Federal Register citation: FR

Other Comments (or details on any Question above):

AI and CMISS are classified as Privacy Act Systems of Records. The notice to cover both systems will be published in the Federal Register by October 30, 2010. Information on this notice can be found at this website: <http://www.hud.gov/offices/cio/privacy/fedreg.cfm>

Section 2.4 – Employee Database Subsystem (EDSS) PIA - FINAL

Program Area: HUD OIG Human Resources

Program Area Manager: Derek Fitzgerald 202.402.4965 dfitzgerald@hudoig.gov

IT Project Leader: James L. Williams, 202.314.5476 jlwilliam@hudoig.gov

For IT Systems:

- **Name of system:** EDSS
- **OMB Unique Project Identifier #:** N/A
- **System Code:** N/A

For Information Collection Requests:

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

Question 1: Provide a brief description of what personal information is collected: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

The personal information collected will serve as an active Employee Directory inclusive of HUD OIG employees. The data contained on each employee is specified in the below table. HUD OIG also utilizes the system as a management tool to manage OIG staff resources and its office locations. The system will include manually inputted information by the HR Office, which pertains to HR functions (i.e., new employee, separated employee status). Inputted information comes from personnel reports from the Bureau of Public Debt (BPD). BPD serves as the OIG’s HR servicing office. EDSS feeds staffing information to CMISS.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

<input checked="" type="checkbox"/>	Name (Last, First, Middle)
<input type="checkbox"/>	Social Security Number (SSN)
<input checked="" type="checkbox"/>	Other identification number (specify type): HUD System ID Number
<input type="checkbox"/>	Birth date (DOB)
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
<input type="checkbox"/>	Personal e-mail address
<input type="checkbox"/>	Fingerprint/ other “biometric”
<input checked="" type="checkbox"/>	Other (specify): Alias, Personal Cell Phone, Work Phone, Signature, Photograph, Active Directory User Name
<input type="checkbox"/>	None
<input type="checkbox"/>	Comment:

Personal/ Sensitive Information:

	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history:
	Education level
	Medical history/ information
	Disability
	Criminal record (Prior Arrest, Date History Checked, Scanned Document/Photograph, Contact Agent)
	Other (specify):
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)? All HUD OIG laptops have FIPS 140-2 approved hard drive encryption implemented.		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? VPN		
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department? Yes, the policy for utilizing remotes access is explained within the HUD OIG Rules of Behavior.		
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Yes, the policy that explains the practices for downloading and local storage of is found in the HUD OIG Rules of Behavior.		
Comment:		

Question 3: Type of electronic system or information collection.

Fill out Section A, B, or C as applicable.

- A. If a new electronic system (or one in development):** Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?
No. If yes, fill out subsections a, b, and c.

Yes		Yes	No
	a. Does the system require authentication?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b. Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c. Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
No			
Comment			

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?	Yes	No
	<input type="checkbox"/>	<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. If an existing electronic system:** Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (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 new Request that will collect data that will be in an automated system? No. 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.

<input checked="" type="checkbox"/>	Yes, this is a new ICR and the data will be automated
<input type="checkbox"/>	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	Comment:

Mark any that apply: Specify LOB applicable to response under question 1.

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
	Other (specify):
	Comment:

Other lines of business (specify uses):

X	Resource Management tool on OIG employees/office locations

Question 4: Will you share the information with others? Yes. (e.g., another agency for a programmatic purpose or outside the government)?

Mark any that apply:

<input checked="" type="checkbox"/>	Federal agencies? Department of Justice
<input type="checkbox"/>	State, local, or tribal governments?
<input type="checkbox"/>	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
<input type="checkbox"/>	FHA-approved lenders?
<input type="checkbox"/>	Credit bureaus?
<input type="checkbox"/>	Local and national organizations?
<input type="checkbox"/>	Non-profits?
<input type="checkbox"/>	Faith-based organizations?
<input type="checkbox"/>	Builders/ developers?
<input type="checkbox"/>	Others? (specify):
<input type="checkbox"/>	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)?

<input type="checkbox"/>	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
<input checked="" type="checkbox"/>	No, they can’t “opt-out” – all personal information is required
<input type="checkbox"/>	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?

- **Records are maintained in a secure computer network, and in locked file cabinets or in metal file cabinets in rooms with controlled access.**

Mark any that apply and give details if requested:

<input checked="" type="checkbox"/>	System users must log-in with a password – <ul style="list-style-type: none"> • Users must login into the network using a user name and password. Access is further restricted by role based access control (RBAC). Application access is further restricted to individual screens and fields.
-------------------------------------	---

	When an employee leaves: How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)?
X	<ul style="list-style-type: none"> 1 week. MAC Delete Request How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <ul style="list-style-type: none"> HR staff searches for the user and ensures their employee status has been changed to separated or retired.
X	Are access rights selectively granted, depending on duties and need-to-know? <ul style="list-style-type: none"> Yes. Spell out acronym RBAC. 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: 1 user Limited/restricted access rights to only selected data: 587 users
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? Yes. (explain your procedures, or describe your plan to improve): <ul style="list-style-type: none"> Data Backups: Incremental backups are performed nightly and full backups are performed weekly and the tapes are stored in locked file cabinet in server room. Refer to HUDOIG-SOP-030, Archival of AutoAudit(AA)/Auto Investigation (AI) Data
	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? N/A. Explain the existing privacy protections, or your plans to improve:
X	Other methods of protecting privacy (specify): <ul style="list-style-type: none"> All laptops have hardware encryption on them. Also any communication outside HUD OIG space is encrypted.
X	Comment: <ul style="list-style-type: none"> Additionally, when users are working from a remote location they remotely access EDSS through an encrypted VPN.

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):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name (Date of Birth, Address, Phone Number)
	Home address
	Home telephone

	Personal e-mail address
	Other (specify):
X	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes No (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

If yes, provide the Federal Register citation: FR

Other Comments (or details on any Question above):

Section 3: Summary

HUD OIG maintains one General Support System called DCE. Within this DCE there are four subsystems, AutoAudit, Hotline, CMISS, and EDSS. Each of these applications to some degree contains PII data (as documented in its corresponding sections above). The PII data that is contained within each subsystem is protected by certain security controls implemented within each of the subsystems. Each subsystem will inherit other security controls that are provided by DCE. These security controls are documented in the DCE System Security Plan.

SECTION 4: DETERMINATION BY THE PRIVACY OFFICE

The PIAs illustrated above were submitted by IG to reflect the current privacy posture of IG's DCE and are approved by the Privacy Office as having the appropriate administrative and security safeguards in place for assuring privacy protection. This information is also reflected in Question #6 of each PIA. Based on the information supplied for each PIA, the risk level assigned to the DCE and its subsystems is low.

Threats: unauthorized access to the DCE and subsystems.

Mitigation / Countermeasures: Access to DCE and subsystems are controlled; users must have a profile/password to log in. All records are maintained in a secure facility with access limited to only authorized personnel or authorized and escorted visitors. Role-based access controls: The level of access granted is dependent upon a person's job responsibilities within IG. Security: The DCE is a secure web based application; Each user is provided with user identification and password and system privileges are configured based on the user's role, approval level, delegations, and special permissions. Technical controls associated with "need to know" and "least privilege" ensure that users have no more privileges to data than required to conduct their official duties. The DCE also completed its Certification and Accreditation in September 2009.

Due to the vast amount of personal / sensitive information contained in the DCE subsystems, the Office of IG will periodically review the privacy controls in place for each system and update the PIA to record any major functionality requirements that creates a privacy risk.