

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

---

**Chief Financial Officer**

**HUD Integrated Financial Management Improvement  
Project (HIFMIP)**

Privacy Impact Assessment

**July 2006**

## DOCUMENT ENDORSEMENT

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

### ENDORSEMENT SECTION

Please check the appropriate statement.

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

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

[/s/ MARY KOHLMEIER](#)

**SYSTEM MANAGER**

Director, Financial Systems Acquisition and  
Development Division  
Office of the Chief Financial Officer  
U. S. Department of Housing and Urban Development

[10/16/06](#)

**Date**

[/s/ GAIL B. DISE](#)

**PROGRAM AREA MANAGER**

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

[10/16/06](#)

**Date**

**DEPARTMENTAL PRIVACY ADVOCATE**

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

**Date**

[/s/ JEANETTE SMITH](#)

**DEPARTMENTAL PRIVACY ACT OFFICER**

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

[10/23/06](#)

**Date**

# TABLE OF CONTENTS

<b>DOCUMENT ENDORSEMENT .....</b>	<b>2</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>SECTION 1: BACKGROUND.....</b>	<b>4</b>
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
<b>SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....</b>	<b>7</b>
Question 1: Provide a brief description of what personal information is collected.....	7
Question 2: Type of electronic system or information collection.....	8
Question 3: Why is the personally identifiable information being collected? How will it be used? .....	10
Question 4: Will you share the information with others? .....	11
Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?.....	11
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	12
Question 7: If privacy information is involved, by what data elements can it be retrieved?...	13
<b>SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE .....</b>	<b>13</b>

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
PRIVACY IMPACT ASSESSMENT (PIA) FOR:  
“HUD INTEGRATED FINANCIAL MANAGEMENT IMPROVEMENT PROJECT”  
(OMB Unique Identifier: 025-00-01-01-01-1050-00-402-124 and PCAS # 411740)  
July 2006**

**NOTE:** See Section 2 for PIA answers, and Section 3 for Privacy Advocate’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](http://www.usdoj.gov/foia/privstat.htm) 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](http://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) ([http://www.usdoj.gov/oip/foia\\_updates/Vol\\_XVII\\_4/page2.htm](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 \(HUD Handbook 1327.1 at www.hudclips.org\)](http://www.hudclips.org));
- [E-Government Act of 2002](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf) 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](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](http://www.whitehouse.gov/omb/egov/pres_state2.htm));
- [Federal Information Security Management Act of 2002](http://uscode.house.gov/search/criteria.php) (which superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at [Title 44 U.S. Code chapter 35 subchapter II](http://uscode.house.gov/search/criteria.php) (<http://uscode.house.gov/search/criteria.php>); and
- [OMB Circular A-130, Management of Federal Information Resources, Appendix I](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) ([http://www.whitehouse.gov/omb/circulars/a130/appendix\\_i.pdf](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](http://www.usdoj.gov/foia/privstat.htm), as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The [E-Government Act of 2002](#) requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

## **Why is the PIA Summary Made Publicly Available?**

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

## SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Advocate in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

**Program Area:** Office of the Chief Financial Officer

**Subject matter expert in the program area:** Gail B. Dise, Deputy Assistant Chief Financial Officer, Office of the Chief Information Officer, (202) 708-1757 Ext. 3749

**Program Area Manager:** Mary Kohlmeier, Director, Financial System Acquisition and Development Division, Office of the Chief Financial Officer, (202) 708-2721 Ext. 3853

**IT Project Leader:** TBD

### For IT Systems:

- **Name of system:** HUD Integrated Financial Management Improvement Project
- **PCAS #:** 00411740
- **OMB Unique Project Identifier #:** 02500010101105000402124
- **System Code:**

### For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

### Question 1: Provide a brief description of what personal information is collected.

The Office of the Chief Financial Officer (OCFO) is charged with developing and maintaining an integrated accounting and financial management system. This system must include financial reporting capability and internal controls that comply with applicable laws, regulations, and standards. The system will contain sensitive and personal information; such as, financial data, limited personnel data, vendor/ customer data, and control data. It will also contain confidential data concerning Internal Revenue Service 1099 tax form records.

Although the Department's current accounting system, "HUD Central Accounting Program System – HUDCAPS" has been effective, it is costly to maintain and does not meet all of HUD's financial reporting needs. As a result of these deficiencies, the OCFO has determined that the HUD Integrated Financial Management Improvement Project (HIFMIP) is the best solution to assist HUD with meeting its financial and budgetary needs more efficiently and effectively.

This initiative will provide HUD with an enterprise-wide financial management system that is compliant with all laws and regulations. The new core financial system will enable HUD to collect, record and maintain all financial data in a single integrated system and have available for HUD management to oversee their programs and external stakeholders for consolidated reporting requirements. This new system will eliminate the need for complex interfaces and will leverage web technology to provide on-line real-time reporting capability to end-users. The end result will be more efficient business processes and more accessible information for decision-makers throughout the Department. Since HIFMIP is not expected to replace HUDCAPS and/

or be implemented until Budget Year 2009 the PIA will need to be revisited and updated upon implementation to expand on the systems usability and to incorporate any changes.

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 Contract recipient and User Names
<input checked="" type="checkbox"/>	Social Security Number (SSN) .
<input checked="" type="checkbox"/>	Other identification number (specify type): User IDs and TINs
	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
	Comment:

**Personal/ Sensitive Information:**

	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Recipients and employees bank names bank account information
	Employment history:
	Education level
	Medical history/ information
	Disability
	Criminal record
	Other (specify):
	None
	Comment:

**Question 2: 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)? **If**



**B. yes, fill out sections a, b, and c.**

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

**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	<b>Conversion:</b> When paper-based records that contain personal information are converted to an electronic system
N/A	<b>From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable):</b> When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
N/A	<b>Significant System Management Changes:</b> 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	<b>Merging Databases:</b> 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	<b>New Public Access:</b> 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	<b>Commercial Sources:</b> 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	<b>New Inter-agency Uses:</b> When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
N/A	<b>Business Process Re-engineering:</b> When altering a business process results in significant new uses, disclosures, or additions of personal data
N/A	<b>Alteration in Character of Data:</b> 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)

**C. 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 <u>new</u> or <u>automated</u> )
	Comment:

**Question 3: Why is 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
X	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

**Rental Housing Assistance:**

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

**Grants:**

	Grant application scoring and selection – if any personal information on the grantee is included
X	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:**

X	Employee payroll or personnel records
X	Payment for employee travel expenses
X	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
X	Other (specify): The system is designed to meet internal and external accounting and budgetary requirements. The current software system will be adapted to meet enterprise wide requirements for the new integrated Departmental core financial system requirements.
	Comment:

**Other lines of business (specify uses):**


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

Mark any that apply:

X	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
X	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
X	Others? (specify): Department of Treasury, Internal Revenue Service, Federal Agency for administrative or salary offset procedures, GAO, Department of Justice, US Attorney, Debt Collection Agency, Resolution Trust Corporation
X	Comment: Only GAO for audit purposes or OIG for audit controls when deemed appropriate.

**Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?**

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
X	No, they can’t “opt-out” – all personal information is required
	Comment:

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

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

Mark any that apply and give details if requested:

<b>X</b>	System users must log-in with a password. User-Identifications are created for approved individuals and passwords are created in accordance with HUD's System Password Policy
	When an employee leaves: <ul style="list-style-type: none"> <li>• How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? This user is terminated from the system in 1 day</li> <li>• How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): The User ID is Deleted user information from system. Notification is submitted to the systems Administration requested that the user be deleted from the system and the users ID is no longer identified in this HIFMIP user administration module</li> </ul>
<b>X</b>	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"> <li>• Full access rights to all data in the system:</li> <li>• Limited/restricted access rights to only selected data: Only users whose duties require access to the system are granted on a need-to-know basis. Additionally, users will be restricted to only the level of system access needed to complete his/her job. The final system design and configuration will determine the total number of authorized users.</li> </ul>
<b>X</b>	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): User Security physical information is safeguarded in a secured room within the HUD building. Electronic files are protected via user profiling and passwords.
<b>X</b>	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: The information residing in the new financial system will be transferred to the data warehouse. The OCFO is responsible for protecting the privacy of data that will come from the new system.
<b>X</b>	Other methods of protecting privacy (specify):
	Comment:

**Question 7: If privacy information is involved, by what data elements can it be retrieved?**

Mark any that apply:

<input checked="" type="checkbox"/>	Name: Contract recipient and User Names
<input checked="" type="checkbox"/>	Social Security Number (SSN)
<input checked="" type="checkbox"/>	Identification number (specify type): User IDs and TINs
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
<input checked="" type="checkbox"/>	Other (specify): Bank accounts #'s
	None
	Comment:

**Other Comments (or details on any Question above):**

**SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE**

While the implementation of HIFMIP is not until 2009, the OCFO has a comprehensive Security Plan in place to ensure protection of the personal identifiable information. Additionally, strict access and administrative controls have been identified as part of question #6 and will be revisited and updated upon implementation to expand on the systems usability and to incorporate any changes. Because of the personal and sensitive nature of the information contained in the system we will annually monitor the development of HIFMIP and its related business processes to ensure that adequate privacy protections are applied.