

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

**Office of Administration,
HR Management Information &
Enterprise Resource Management
Planning Systems Staff**

**HUD INTEGRATED HUMAN RESOURCES AND
TRAINING SYSTEM (IHRTS) DATASTORE**

Privacy Impact Assessment

September 2009

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **HUD Integrated Human Resources and Training System (HHRTS) Datastore (P162D)**. 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/ Sharman R. Lancefield

SHARMAN R. LANCEFIELD - SYSTEM OWNER
Deputy Assistant Secretary for Human Resources
Office of Administration

10/19/2009

Date

/s/ Charles Butler

CHARLES BUTLER
Director
HR Management Information & Enterprise Resource
Management Planning Systems Staff
Office of Administration

10/19/2009

Date

/s/ Donna Robinson-Staton

DEPARTMENTAL PRIVACY ACT OFFICER
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

11/12/2009

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....	7
Question 1: Provide a brief description of what personal information is collected.	7
Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?	8
Question 3: Type of electronic system or information collection.....	9
Question 4: Why is the personally identifiable information being collected? How will it be used?	10
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	11
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)?	12
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 element(s) is it retrieved from the system?.....	13
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	13

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
HUD INTEGRATED HUMAN RESOURCES AND TRAINING SYSTEM (HIHRTS)
DATASTORE**

September 30, 2009

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 superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at [Title 44 U.S. Code chapter 35 subchapter II](#) (<http://uscode.house.gov/search/criteria.php>); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).
- 2. Existing Systems:** Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA):

Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The Privacy Act of 1974, as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

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

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

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

Program Area: Office of Administration, HR Management
Subject matter expert in the program area: Denis McGurin
Program Area Manager: Charles Butler
IT Project Leader: Denis McGurin

For IT Systems:

- **Name of system:** HUD Integrated Human Resources and Training System (HIHRTS) Datastore
- **PCAS #:** 000202750
- **OMB Unique Project Identifier #:** 025-00-01-07-01-1520-00
- **System Code:** P162D

For Information Collection Requests:

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

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

The HIHRTS Datastore does not process transactions and does not collect information. The information contained in HIHRTS Datastore is received by a nightly download from the transactional HIHRTS system at the Department of Treasury. The data in P162D is used to query information for reporting and interfacing with other HUD applications. Data include human resources information for personnel action processing, hiring, performance management and workforce analysis and is of HUD Employees, former employees, and applicants for employment. There is no information maintained from the public or from government contractors and consultants for this system.

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:

Yes	Name
Yes	Social Security Number (SSN) .
Yes	Other identification number (specify type): “H” Id
Yes	Birth date
Yes	Home address
Yes	Home telephone
Yes	Personal e-mail address
No	Fingerprint/ other “biometric”
	Other (specify):

	None
	Comment:

Personal/ Sensitive Information:

Yes	Race/ ethnicity
Yes	Gender/ sex
Yes	Marital status
Yes	Spouse name (If employee includes spouse as an Emergency Contact.)
No	# of children
Yes	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Salary
Yes	Employment history: HUD only unless the employee was previously employed by an organization using Treasury's HR Connect.
Yes	Education level
No	Medical history/ information
Yes	Disability
No	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)? Restricted to use via HUD Intranet Only authorized users are allowed access to HIRTS via an individual user id and password. All passwords are stored in encrypted form in the database. The system is only accessible through HUD network.		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? VPN Since the system is only accessible through HUD network; only way to access is remotely is to first establish a VPN connection to HUD network.		

<p>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/Starbucks) or is remote access permitted from all areas outside the Department?</p> <p>Policy of HR is to access from a HUD Office unless using VPN and then not in a public place.</p>
<p>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)?</p> <p>HUD IT Security Handbook 2400.25, 5.2.17 and Rules of Behavior for Remote Access at: http://hudatwork.hud.gov/po/i/it/remoterules116c.pdf</p>
<p>Comment:</p>

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"/>

B 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)

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.

	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:

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

Rental Housing Assistance:

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

Grants:

N/A	Grant application scoring and selection – if any personal information on the grantee is included
N/A	Disbursement of funds to grantees – if any personal information is included
N/A	Other (specify):
N/A	Comment:

Fair Housing:

N/A	Housing discrimination complaints and resulting case files
N/A	Other (specify):
N/A	Comment:

Internal operations:

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

Yes	Federal agencies? The HHHRTS Datastore has the capability to produce the MD 715 report tables that all Federal agencies provide to the EEOC. This data is in aggregate and does not report information on individual employees. No data is provided back to the Treasury system or origin.
No	State, local, or tribal governments?

No	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
No	FHA-approved lenders?
No	Credit bureaus?
No	Local and national organizations?
No	Non-profits?
No	Faith-based organizations?
No	Builders/ developers?
No	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
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 7: 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 to 1 week • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): Primary, The HIHRTS Datastore Security Administrator has the Datastore access terminated. Secondary, HUDGONE process that terminates the H-ID will terminate LAN and therefore HIHRTS Datastore access.
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: 6 • Limited/restricted access rights to only selected data: 0
N/A	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):

	Disks and tapes are not outputs of the HIHRTS Datastore. Users can print reports or store report files. All users are required to take security and privacy training.
X	<p>If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: The system and information owner of data is responsible for protectin the data that interfaces with it systems. Safeguard information in information systems is also communicate in the mandatory Security awareness training annually.</p> <p>Information in HIHRTS Datastore is not updated within the HIHRTS Datastore and is not sent back to Treasury.</p>
N/A	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

Yes	Name:
Yes	Social Security Number (SSN)
Yes	Identification number (specify type): "H" Id
Yes	Birth date
Yes	Race/ ethnicity
Yes	Marital status
Yes	Spouse name
Yes	Home address
Yes	Home telephone
Yes	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

[The users of HIHRTS Datastore are the Department of Housing and Urban Development \(HUD\) staff.](#)

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

[The HIHRTS Datastore require privacy protection due to the collection, use and maintenance of sensitive and personally identifying information. Based on the information supplied by the](#)

Program Office and my assessment of the PIA I have determined that there are adequate protection and security controls in place to adequately protect the systems data. Additionally this system is classified as a Privacy Act System of Records, HUD-34: Pay and Leave Records of Employee, which prohibits the disclosure of records from the system without an exception for disclosure, and prior publication. You may refer to HUD's privacy webpage to review the existing SORN in full text: http://www.hud.gov/offices/cio/privacy/sorns/hud_34.cfm