# Department of Housing and Urban Development

# Public and Indian Housing Information Technology

## Information Security Program

## Web Access Security Sub-System

## Privacy Impact Assessment

October 2005

## DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the Web Access Security Sub-System (WASS). This document has been completed in accordance with the requirements set forth by the Federal Information Security Management Act of 2002 (FISMA), Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Public and Indian Housing (PIH) Information Technology (IT) Office.

MANAGEMENT ENDORSEMENT

Please check the appropriate statement.

__X__ The document is accepted.
______ The document is accepted pending the changes noted.
______ The document is not accepted.

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

**/s/ Eric M. Stout** — **Dec. 14, 2005**
**Departmental Privacy Advocate** — **Date**

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

**/s/ Jeanette Smith** — **Dec. 14, 2005**
**Departmental Privacy Act Officer** — **Date**

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

## TABLE OF CONTENTS

## U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT (HUD) PRIVACY IMPACT ASSESSMENT (PIA) FOR:

**Web Access Security Sub-System (WASS)**
**(For Information Collections: OMB Control #:** TBA)
**(For IT Systems: OMB Unique Identifier:** TBA)
**PCAS #** REAC - 307904
**October 2005**

## SECTION 1. BACKGROUND

### Importance of Privacy Protection – Legislative Mandates

The Department of Housing and Urban Development (HUD) is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, the beneficiaries of HUD programs and business partners, and its own employees. These individuals have a right to expect that HUD will collect, maintain, use, and disseminate personally identifiable information (PII) only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended, affords individuals the right to privacy in records that are maintained and used by Federal agencies (See http://www.usdoj.gov/foia/privstat.htm; see also HUD Handbook1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988, which amends the Privacy Act of 1974, 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 public information maintained by Federal agencies, 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 PIAs on their 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 supersedes 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
- Office of Management and Budget (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 PII will be restricted to those staff who need the data to carry out their duties. Such staff will be held accountable for ensuring privacy and confidentiality of the data.

### What is the PIA Process?

The PIA process evaluates issues related to the privacy of PII in electronic systems. (See background on PIAs and the seven questions that need to be answered at: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm.) PII is defined as information that identifies an individual by name, address, social security number (SSN), or identifying number or code; or by other personal/ sensitive information such as race, marital status, financial information, home telephone number, or personal e-mail address. Of particular concern is the combination of multiple identifying elements. For example, knowing the name, SSN, birth date, and financial information would pose greater risk to privacy than knowing only the name and SSN.

The PIA:

- Identifies the type of PII in the system and the system's ability to combine multiple identifying elements on an individual,
- Identifies who has access to that information and whether they have full access or limited access rights, and
- Defines the administrative controls which ensure that only the information necessary and relevant to HUD's mission is in the system.

### Who Completes the PIA?

The program area system owner and the information technology (IT) project leader work together to complete the PIA. The system owner describes what personal data types are collected, how the data are 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 to PII.

### When is a PIA Required?

1. **New Systems.** According to OMB requirements, a PIA is required for any new system, including major and non-major systems, containing personal information on members of the public.

2. **Existing Systems.** A PIA is required where significant modifications have been made to an existing system that involve personal information on members of the public or may create a new privacy risk.

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, a PIA is required.

### What are the Privacy Act Requirements?

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, by some other identifying number or symbol, or by other particular identifiers assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems and for information collection requests that are automated. Therefore, a relationship exists between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notice requirement (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 (OCIO).

**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 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

**Program Area:** Office of Public and Indian Housing (PIH) – Information Technology (IT)
**Subject Matter Expert in the Program Area:** Gary Faeth
**Program Area Manager:** Gary Faeth
**IT Project Leader:** Hitesh Doshi

For IT Systems:

- **Name of system:** Web Access Security Sub-System (WASS)
- **PCAS #:** REAC – 307904
- **OMB Unique Project Identifier #:** TBA

For Information Collection Requests:

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

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

WASS is a major application designed to protect PIH Real Estate Assessment Center's (REAC) database by providing a secure connection, identification and authentication services, and access control for over 25 HUD systems managed by the PIH IT and the Office of Housing - Single Family Housing and Multifamily Housing. WASS verifies and validates user's identity, controls user access to certain systems, and allows only the appropriate privileges for each user. WASS does collect user social security numbers and mother's maiden name. These are used strictly for authentication of users when users request password resets, etc.

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

**Personal Identifiers:**

| | |
|---|---|
| X | Name: |
| X | Social Security Number (SSN): full SSN is collected, only last 4 digits are displayed and used |
| | Other identification number (specify type): |
| | Birth date: |
| | Home address: |
| | Home telephone: |
| | Personal e-mail address: |
| | Fingerprint/ other "biometric": |
| | Other (specify): Mother's Maiden name |
| X | None |
| X | Comment: WASS is a management system. WASS provides protection to PIH-REAC's database by providing a secure connection, identification and authentication services, and access control for over 20 HUD systems managed by the PIH-REAC and the Office of Housing - Single Family Housing and Multifamily Housing. The last 4 digits of the SSN and the Mother's Maiden Name are used STRICTLY for authentication of users when they are requesting password resets, etc. |

### Personal/ Sensitive Information:

| | |
|---|---|
| | Race/ethnicity: |
| | Gender: |
| | Marital status: |
| | Spouse name: |
| | Number of children: |
| | Income/financial data (specify type of data, such as salary, Federal taxes paid, bank account number): |
| | Employment history: |
| | Education level: |
| | Medical history/information: |
| | Disability: |
| | Criminal record: |
| | Other (specify): |
| X | None |
| X | Comment: HUD does not use this system to collect, maintain, or disseminate PII from or about individuals. WASS is a management system. WASS provides protection to PIH-REAC's database by providing a secure connection, identification and authentication services, and access control for over 20 HUD systems managed by the PIH-REAC and the Office of Housing - Single Family Housing and Multifamily Housing. The last 4 digits of the SSN and the Mother's Maiden Name are used STRICTLY for authentication of users when they are requesting password resets, etc. |

**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)?

| | |
|---|---|
| | Yes |
| X | No |
| X | Comment: WASS is an existing system in the operational phase of its system development life cycle. PIH IT is conducting this initial PIA on the system in recognition of the importance of privacy protection and as part of its Department privacy best practices. |

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 become 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 new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology) |
| 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 only a name and address) |

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

## Question 3: Why is the PII being collected? How will it be used?

Mark any that apply:

### Homeownership:

| | |
|---|---|
| | Credit checks (eligibility for loans) |
| | Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information |
| | Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD) |
| | Loan default tracking |
| | Issuing mortgage and loan insurance |
| | Other (specify): |
| X | None |

### Rental Housing Assistance:

| | |
|---|---|
| | Eligibility for rental assistance or other HUD program benefits |
| | Characteristics on those receiving rental assistance (for example, race/ethnicity, number of children, age) |
| | Property inspections |
| | Other (specify): |
| X | None |

### Grants:

| | |
|---|---|
| | Grant application scoring and selection – if any personal information on the grantee is included |
| | Disburse funds to grantees – if any personal information is included |
| | Other (specify): |
| X | None |

### Fair Housing:

| | |
|---|---|
| | Housing discrimination complaints and resulting case files |
| | Other (specify): |
| X | None |

### Internal Operations:

| | |
|---|---|
| | Employee payroll or personnel records |
| | Payment for employee travel expenses |
| | Payment for services or products (to contractors) – if any personal information on the payee is included |
| | Computer security files – with personal information in the database, collected in order to grant user IDs |
| X | Other (specify): WASS data consists of user IDs and passwords. This data is properly protected, so that only authorized users can use this information to gain access to over 25 HUD systems. WASS verifies and validates user's identity, controls users assess to certain systems, and allows only the appropriate privileges for each user. |
| | None |

### Other Lines of Business (specify uses):

| | |
|---|---|
| X | Other: WASS provides user authentication and authorization for access to over 25 HUD Web-based information systems as noted above. PII collected is maintained in a encrypted database and is used solely for identification and authentication when users call in for assistance with their accounts. |
| | |
| | |

**Question 4: Will you share the PII with others?**

For example, another agency for a programmatic purpose or outside the government. Mark any that apply.

| | |
|---|---|
| | Federal agencies (specify): |
| | State, local, or tribal governments |
| | Public Housing Agencies 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):<br>While WASS interfaces with the organizations listed below, WASS does not share PII with these groups.<br>• Office of Information Technology (OIT)<br>• Internet Services Group (ISG)<br>• The Real Estate Assessment Center<br>• Office of Multifamily Housing<br>• Office of Public and Indian Housing<br>• Office of Single Family Housing |
| | None |
| X | Comment: |

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

| | |
|---|---|
| X | Yes. They can "opt-out" by declining to provide private information or by consenting only to particular use. |
| | No. They can't "opt-out" – all personal information is required. |
| X | Comment: PII collected is maintained in a encrypted database and is used solely for identification and authentication when users call in for assistance with their accounts. It is possible for users to provide a false SSN which is not a problem as it is used strictly for authentication purposes, and any 9 digit number can be used as long as it is in the proper format. |

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):________N/A________________________________

_______________________________________________________________________________

_______________________________________________________________________________

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

Mark any that apply and give details if requested (if not applicable, mark N/A).

| | |
|---|---|
| X | System users must log in with a password |
| N/A | When an employee leaves:<br>How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)?<br>How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): |
| X | Are access rights selectively granted, depending on duties and need-to-know? YES<br>If yes, specify the approximate number of authorized users who have either:<br>• Full access rights to all data in the system (specify number): 24<br>• Limited/restricted access rights to only selected data (specify number) |
| 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): |
| N/A | If data from your system are 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 | Comment: PII collected is maintained in a encrypted database and is used solely for identification and authentication when users call in for assistance with their accounts. |

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

Mark any that apply.

| | |
|---|---|
| X | Name: |
| X | Social Security Number (SSN): |
| | Identification number (specify type): |
| | Birth date: |
| | Race/ethnicity: |
| | Marital status: |
| | Spouse name: |
| | Home address: |
| | Home telephone: |
| | Personal e-mail address: |
| | None |
| X | Comment: PII collected is maintained in a encrypted database and is used solely for identification and authentication when users call in for assistance with their accounts. Social Security Numbers can only be retrieved by highest level admin users. WASS does not constitute a Privacy Act System of Records and does not contain privacy information that can be retrieved by data element. |

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

## SECTION 3. DETERMINATION BY HUD PRIVACY ADVOCATE

Lisa Schlosser Date
Chief Information Officer
U.S. Department of Housing and Urban Development

Jeanette Smith Date
Department Senior Privacy Act Officer
Office of the Chief Information Officer
U.S. Department of Housing and Urban Development

Eric M. Stout Date
Department Privacy Advocate
Office of the Chief Information Officer
U.S. Department of Housing and Urban Development