

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

---

**Office of Administrative Law Judges**

Administrative Law Judge  
(ALJ) Monitor System  
Privacy Impact Assessment

May 2005

**DOCUMENT ENDORSEMENT**

I have carefully assessed the Privacy Impact Assessment (PIA) for Administrative Law Judge system. 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.

**MANAGEMENT ENDORSEMENT**

**Please check the appropriate statement.**

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

**/s/ Eric M. Stout**

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

**May 3, 2005**

**Date**

**/s/ Jeanette Smith**

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

**May 3, 2005**

**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 Requirement?.....	6
Why is a 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 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
For Example: another agency for a programmatic purpose, or outside the government. ....	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 private information is involved, by what data elements can it be retrieved? ...	12
<b>SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE .....</b>	<b>13</b>

**APPROVED/ FINAL**

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
PRIVACY IMPACT ASSESSMENT (PIA) FOR:  
“ADMINISTRATIVE LAW JUDGE (ALJ) CASE  
MONITORING SYSTEM”  
(OMB Unique Identifier N/A and PCAS # 00307820)  
May 2, 2005**

**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://www.whitehouse.gov/omb/egov/pres_state2.htm) requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See [http://www.whitehouse.gov/omb/egov/pres\\_state2.htm](http://www.whitehouse.gov/omb/egov/pres_state2.htm)); 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://www.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 \(http://www.uscode.house.gov/search/criteria.php\)](http://www.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 HUD staff who have been authorized because of their duties; and they will be held accountable for ensuring privacy and confidentiality.

### **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 Requirement?**

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 a 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 Administrative Law Judges, HUD

**Subject matter expert in the program area:** Arthur Liberty, Chief Administrative Law Judge, Office of Administrative Law Judge, HUD, (202) 708-5014

**Program area manager:** Arthur Liberty (see above)

**IT Project Leader:** James S. Pinto, IT Project Manager, Executive Services Information Support Division, HUD, (202) 401-1795, ext 6094; Dawn M. Nance, Director, Executive Services Information Support Division, HUD, (202) 401-1795, ext. 6229

### For IT Systems:

- **Name of system:** Administrative Law Judge (ALJ) Monitor System
- **PCAS #:** 00307820
- **OMB Unique Project Identifier # (if submitting an Exhibit 300 to OMB):** N/A (not a major system, therefore an Exhibit 300 was not submitted to OMB)

### For Information Collection Requests:

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

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

The ALJ Monitor System is a case docketing and tracking system used to account for pleadings, orders and determinations in cases before HUD Administrative Law Judges. Principle uses includes:

- Tracking and accounting for filings (complaints, pleadings, orders and determination) in all cases, both pending and archived;
- Generating statistical reports for other HUD offices (FHEO and OGC) and the Congress;
- Responding to Freedom of Information Act requests from the public;
- Providing the chief judge management information necessary to assess workload, assign incoming cases and monitor case progress;
- Allow individual judges to monitor the progress of assigned cases; and
- Provide ready access to case docketing information to support staff to enable timely response to complainants, government and private counsel, and defendants concerning the status of a particular case.

The system streamlines the internal processes and helps the Department meet the statutory and regulatory requirements by supporting the necessary case administration functions.

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)
<input checked="" type="checkbox"/>	Other identification number (specify type): Case numbers
<input checked="" type="checkbox"/>	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
<input checked="" type="checkbox"/>	Comment: ALJ contain Private and sensitive information relevant to pending and resolved cases by Administrative Law Judges

**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
<input checked="" type="checkbox"/>	Medical history/ information
<input checked="" type="checkbox"/>	Disability
	Criminal record
	Other (specify):
	None
<input checked="" type="checkbox"/>	Comment: ALJ contain Private and sensitive information relevant to pending and resolved cases by Administrative Law Judges

**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
<input checked="" type="checkbox"/>	No

**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):

X	<b>Conversion:</b> When paper-based records that contain personal information are converted to an electronic system
X	<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
X	<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)
X	<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
X	<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)
	(Specify)

**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> )
X	Comment: <b>This Monitor system has been in existence for 6 years and reengineered from a previous case tracking system.</b>

**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)
X	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)
X	Loan default tracking
X	Issuing mortgage and loan insurance
X	Other (specify): Information collected for ALJ case resolution.
	Comment:

**Rental Housing Assistance:**

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

**Grants:**

X	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:**

X	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
X	Computer security files – with personal information in the database, collected in order to grant user IDs

<input checked="" type="checkbox"/>	Other (specify):
	Comment:

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


**Other related information pertaining to the Department (please specify):**

	Other (specify):
	Comment:

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

**For Example: another agency for a programmatic purpose, or outside the government.**

Mark any that apply:

<input checked="" type="checkbox"/>	Federal agencies? (specify):
<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?
<input checked="" type="checkbox"/>	Builders/ developers?
	Others? (specify):
	Comment:.

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

	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): \_\_\_\_\_

**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"> <li>• How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? <b>1 day.</b></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): <b>Former employees access is first deleted from the HUD infrastructure and then specifically from this Monitor system. Also the employee relinquishes his ID card that granted physical access to the building facility and the ALJ office suite.</b></li> </ul>
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the # of authorized users who have either: <b>Yes, 6 users have access to ALJ, the system is controlled by limited access at various levels on and need-to-know basis.</b> <ul style="list-style-type: none"> <li>• Full access rights to all data in the system (specify #)? <b>Limited/ restricted access rights to only selected data (specify #)? Restricted access to the system on a need-to-know-basis.</b></li> </ul>
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): <b>N/A only reports. Yes, all electronic data are contained in HUD IT infrastructure servers. Any hardcopy documents are maintained in locked cabinets in the secured ALJ suite of offices.</b>
X	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: <b>Data are not shared with other systems</b>
	Other methods of protecting privacy (specify):
X	Comment: <b>The system ensures the privacy of sensitive information by controlling access at various levels on and need-to-know basis.</b>

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

Mark any that apply:

X	Name
X	Social Security Number (SSN)

X	Identification number (specify type):
X	Birth date
X	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
X	Home telephone
X	Personal e-mail address
	Other (specify):
	None
X	Comment: The system ensures the privacy of personal information by controlling access at various levels on and need-to-know basis

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

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

The data contained in AJI is sensitive and proprietary and relates to pending and resolved cases by Administrative Law Judges. Final dissemination of ALJ information is done in accordance with related regulation of archiving information and the Freedom of Information Act (FOIA), thereby adhering to Archive and FOIA requirements.

Because ALJ contains sensitive information, we will annually monitor this system and related business processes to ensure that adequate privacy protections continue to be in place.