

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

---

**Office of the Chief Financial Officer**

**Nortridge Loan Accounting System (NLS/LAS-A21)**

Privacy Impact Assessment

**August 23, 2006**

## DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for [**Insert Name of IT System and/ or Information Collection Request**]. 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/ Michael K. Simmons

**SYSTEM MANGER** (Michael K. Simmons, System Accountant, Financial Systems Maintenance Division)  
Office of the Chief Financial Officer  
U.S. Department of Housing and Urban Development

8/23/06

**Date**

/s/ Gail B. Dise

**PROGRAM AREA MANAGER** (Gail B. Dise, Deputy Assistant Chief Financial Officer)  
Office of the Chief Financial Officer  
U.S. Department of Housing and Urban Development

8/23/06

**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.....	9
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)? .....	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 elements can it be retrieved?...	14
<b>SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE .....</b>	<b>14</b>

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT**  
**PRIVACY IMPACT ASSESSMENT (PIA) FOR:**  
**“Loan Accounting System (NLS/LAS – A-21)”**  
**(for IT Systems: OMB Unique Identifier 025-00-01-01-02-1150-00-402-124**  
**and PCAS # 00202740)**  
**August 23, 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 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 \(http://uscode.house.gov/search/criteria.php\)](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:** Michael K. Simmons, System Accountant, Financial Systems Maintenance Division, Office of the Chief Financial Officer, (202) 708-0614 x3738

**Program Area Manager:** Gail B. Dise, Deputy Assistant Chief Financial Officer, Office of the Chief Financial Officer, (202) 708-0614 x3749

**IT Project Leader:** Christopher L. Turner, Computer Specialist, Office of Information Technology, (202) 708-0614 x7126

### For IT Systems:

- **Name of system:** A21 Loan Accounting System –(NLS/LAS-A21)
- **PCAS #:** 00202740
- **OMB Unique Project Identifier #:** 025-00-01-01-02-1150-00-402-124
- **System Code:** A21 NLS/LAS

### For Information Collection Requests:

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

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

The NLS/LAS system processes Multifamily Housing Section 202 Elderly and Handicapped Loan and the 201 Flex Subsidy program activity and maintains loan information from the initial reservation phase, through disbursements and collections on construction loans and finally through repayment of the permanent loans. The system accrues interest and bills for principal and interest due, provides inquiry and ad hoc reporting on outstanding loans, liabilities, monies disbursed by HUD, collected by HUD and due to HUD.

The timeliness and accuracy of the NLS/LAS accounting transactions is critical to the successful generation of the CFO's SF-224 monthly report of cash activity to the U.S. Department of the Treasury. Additionally, The LAS system:

- Maintains the Section 202 and 201 programs' loan information from the initial reservation phase through disbursement and collections on construction projects and through repayment of permanent financing after projects have converted from construction to permanent loan status
- Calculates funds that are applied to the interest and principal amounts due for each loan and
- Provides ability to record penalty and refund transactions for specific projects
- Performs interest accrual processing for project loans in one of the following two ways:

- Accrues interest and applies it based on an amortization schedule or
- Calculates interest using a specific rate charged over a period of time against an outstanding balance
- Bills for principal and interest due
- Provides project and transaction reports
- Provides inquiry and ad hoc reporting on outstanding loan liabilities, disbursements, collections, and receivables
- Incorporates several security features to safeguard against unauthorized use. In addition to user identification (ID) and passwords, the system restricts access to specific functions according to the user's clearance level and program area.

NLS/LAS does not collect personal/ sensitive information subject to the Privacy Act of 1974. The system contains multifamily direct loan financial information only. The specific data collected within the system includes loan attributes of business partners such as interest rate, effective date, term, borrower name, address, and loan number.

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:**

X	Name (Name of business partner, not of an individual borrower is recorded in system)
	Social Security Number (SSN)
X	Other identification number (specify type): <b>Loan Number</b>
	Birth date
	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
X	Other (specify): <b>Includes business address of business partner, not of individuals residence are recorded in system.</b>
	None
X	Comment <b>There is no personal/sensitive information recorded for this program. Only sponsor business information is recorded in system.</b>

**Personal/ Sensitive Information:**

	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history:

	Education level
	Medical history/ information
	Disability
	Criminal record
	Other (specify):
	None
X	Comment: There is no personal/ sensitive information recorded for this program, only sponsor business information is recorded.

**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 yes, fill out subsections a, b, and c.**

	Yes	Yes	No
	a. Does the system require authentication?	<input type="checkbox"/>	<input type="checkbox"/>
	b. Is the system browser-based?	<input type="checkbox"/>	<input type="checkbox"/>
	c. Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input type="checkbox"/>
X	No		
	Comment : OCFO has converted the data from the existing LAS to a COTS package. The implementation date is August 9, 2006. The same type of sponsor business information will be recorded in the COTS package that is currently in the existing system.		

- A. 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.

	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 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
	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	Comment: <u>No personal/ sensitive information is collected in this system.</u>

**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):
X	Comment: <b>No personal/ sensitive information is collected in this system.</b>

**Grants:**

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
X	Comment: <b>No personal/ sensitive information is collected in this system.</b>

**Fair Housing:**

	Housing discrimination complaints and resulting case files
	Other (specify):
X	Comment: <b>No personal/ sensitive information is collected in this system</b>

**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
	Other (specify):
X	Comment: <b>No personal/ sensitive information is collected in this system</b>

**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:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?

	Others? (specify):
X	Comment: <b>The information on each project is not shared with any other sponsor associated with the program.</b>

**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 <b>Personal/ sensitive information is not required or captured in this system</b>
	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	<p><b>System users must log-in with a password</b></p> <p>The application supports access security using User ID and encrypted Passwords to provide authorized users with access. Passwords are periodically changed and rules for length, composition (uppercase/lowercase, numeric) and re-use are dependent upon the individual application controls. Even though the system does not capture personal/ sensitive information, this security process does apply in this system to protect the business information on the project.</p>
---	---

X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> <li>• How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)?</li> </ul> <p>As part of the employees exit process the security officer sign the forms and removes the employees access ability form the system within 1 day of notice.</p> <ul style="list-style-type: none"> <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):</li> </ul> <p>There is an automated workflow process for requesting, establishing, and issuing user accounts. As part of out-processing, for both friendly and unfriendly terminations, employees must checkout with IT Security to close their user account. In addition, the security administrator conducts a quarterly re-validation of users that is forwarded to IT Security (ITSEC) to ensure invalid user accounts are closed.</p>
X	<p>Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:</p> <ul style="list-style-type: none"> <li>• <b>Full access rights to all data in the system:</b></li> </ul> <p>The Office of the Chief Financial Officer (CFO) may grant system access to employees, contractors, clients/customers, and program participants who have a need to utilize CFO major application systems. Users must submit a User Request for ADP Resources, Form 22017 to request access to LAS. Supervisors and the System Security Administrator for appropriate sensitivity level have reviewed all positions. The separation of duties requirement also establishes which level of access an employee will receive.</p> <ul style="list-style-type: none"> <li>• Limited/restricted access rights to only selected data:</li> </ul> <p>Users are assigned to groups that are established with certain levels of access. This will prevent user from accessing areas not assigned to that group.</p>
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve):</p> <p>LAS hardware is located in a secure location under the control of the Computer Services Operations and Maintenance Group (CSOMG).</p> <p>The OCIO Operations staff is responsible for the security of the computer center, software, and all data used or stored there. Additionally, printed output that needs to be transported to its destination is done so via an internal HUD courier service maintained by the HUD Information Technology Service (HITS) contract. For larger reports, the HQ Print Center is utilized. Within the print center, all printouts are uniformly treated as sensitive/proprietary. A single point of contact (manager or above) is assigned a lock-box and lock combination for delivery and receipt of printouts. Printouts not having a lock-box assignment are kept at the print facility and released by print center personnel only upon an approved signature and visual badge inspection. A manual audit log maintains a record of each printout and the signature of the person who received the documents. The document pick-up area has a door with a wire screen at the window opening. The Print Center staff electronically controls access to this area. The other entry to the print center is controlled via card key access. Even though there is <u>no</u> personal/ sensitive information captured in the system, there is a process in place to protect the security</p>

	of the sponsor business information.
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: Even though there is <u>no</u> personal/ sensitive information, the sponsor information that is sent to the Data Mart can't be changed within the Data Mart application (inquiry only). The Data Mart is a repository of financial information in which an ad hoc report writer tool is utilized for creating reports.
	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:

X	Name: (Name of business partner, not of an individual borrower)
	Social Security Number (SSN)
X	Identification number (specify type): Loan #
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
X	Other (specify): Includes business address of business partner, not an individuals residence
	None
X	Comment: No personal/ sensitive information is collected in this system

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

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

NLS/LAS supports the Department's financial reporting requirements in the Multifamily Housing loan receivable and collection area. Also, this application assists HUD to empower its

end users with improved access to Multifamily direct loan financial information, and reduce the workload associated with managing its financial management processes.

The data contained in the NLS/LAS database contains sensitive business information does not include sensitive or personal loan information that's subject to the Privacy Act. There are appropriate security measures in place to ensure the confidentiality of sponsor loan data contained in NLS/LAS.