

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

Office of the Chief Information Officer

ERM-CTS

Privacy Impact Assessment

September 28, 2011

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for ERM-CTS. 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/ Dolores Cole](#)

PROGRAM DIRECTOR

Dolores Cole

[9-27-11](#)

Date

[/s/ Vicky Lewis](#)

PROGRAM AREA MANAGER

Vicky Lewis, Assistant Executive Secretary

[9-27-11](#)

Date

[/s/ Vicky Lewis](#)

IT PROJECT MANAGER

Edith Pembleton

[9-27-11](#)

Date

[/s/ Harold Williams](#)

DEPARTMENTAL PRIVACY ACT OFFICER

Office of the Chief Information Officer

U. S. Department of Housing and Urban Development

[9-27-11](#)

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	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 2: Type of electronic system or information collection.....	8
Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?	10
Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module 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 privacy information is involved, by what data element(s) is it retrieved from the system?.....	13
Question 9: What are the Retention Use and Disposal Practices. Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.....	14
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....	14

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
ELECTRONIC RECORDS MANAGEMENT CORRESPONDENCE TRACKING SYSTEM
(ERM/CTS)

(For IT Systems: OMB Unique Project Identifier: 025-00-01-05-01-1240-00 and
PCAS#: 00663580)
September 28, 2011

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 superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security

regulations at [Title 44 U.S. Code chapter 35 subchapter II \(http://uscode.house.gov/search/criteria.php\)](http://uscode.house.gov/search/criteria.php); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I \(http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf\)](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) 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 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 – Executive Secretariat

Subject Matter Expert in the Program Area: Vicky Lewis, Assistant Executive Secretary

Program Area Manager: Dolores Cole, Director, Executive Secretariat

IT Project Leader: Edith Pembleton, Office of Enterprise Architecture, Office of the Chief Information Officer, (202) 402-6269;

For IT Systems:

- **Name of system:** Enterprise Electronic Records/Correspondence Tracking System (ERM/CTS)
- **PCAS #:** 00663580
- **OMB Unique Project Identifier #:** 025-00-01-05-01-1240-00
- **System Code:** P228
- **Development Date:** September 28, 2011
- **Expected Production Date:** October 3, 2011

For Information Collection Requests:

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

Question 1: Provide a general description of the system that describes: The following questions are intended to define the scope of the information in the system (or information collection), specifically the nature of the information and the sources from which it is obtained.

- a. **What is the personal information being collected?** CTS, Correspondence Tracking System is the automated action and case tracking system that replaces HUD's legacy correspondence tracking system, Automated Correspondence On-line Response Network (ACORN). CTS expand the Department's correspondence electronic capability to accurately report and monitor the status of both correspondence internal to the Department and those received from the public. It gives the department the ability to execute, prioritize and expedite the correspondence workflow more effectively.

FMS2 (FOIA Management System) electronically stores, retrieves, redacts, and prints documents for delivery to FOIA requesters. It also keeps track of FOIA processing statistics and fees, and generates reports on the number, type, and disposition of FOIA requests processed, as required by the U.S. Department of Justice.

Both systems collect personal name, home address, telephone and email address of the writer from the incoming request to be able to respond to the correspondence via system-

generated emails or generated MS Word documents. The system provides access permissions to restrict access if the subject so requires. In addition, CTS users are registered within CTS with Name, HUD email address, and work phone numbers.

- b. **From whom is the information collected (i.e., government employees, contractors, or consultants)?** All persons requesting information from HUD according to the Freedom of Information Act.
- c. **What is the functionality of the system and the purpose that the records and/or system serve?** TBD
- d. **How information is transmitted to and from the system;** Documents will be scanned into the system and also transferred from a former database.
- e. **What are the interconnections with other systems.** N/A
- f. **What specific legal authorities, arrangement, and/or agreement authorize the collection of information (i.e. must include authorities that cover all information collection activities, including Social Security Numbers)?** The Freedom of Information Act of allows legal authorities to request previously unreleased information and documents controlled by the United States government

Question 2: Type of electronic system or information collection.

A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	Yes	No
	<input type="checkbox"/>	<input checked="" 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 this is existing electronic system has the system undergone any changes (since April 17, 2003)? August 2011	Yes	No
	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
If yes, please explain:		

<p>C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA or PIA update (if not applicable, mark N/A):</p>	
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)

<p>D. If an Information Collection Request (ICR): Is this a <u>new</u> Request that will collect data that will be in an <u>automated</u> 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 <u>new</u> request and the collected data will be in an <u>automated</u> system.</p>	
	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: Explain by Line of Business why the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

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

Rental Housing Assistance:

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

Grants:

<input type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Fair Housing:

<input type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Internal operations:

<input type="checkbox"/>	Employee payroll or personnel records
<input type="checkbox"/>	Payment for employee travel expenses
<input type="checkbox"/>	Payment for services or products (to contractors) – if any personal information on the payee is included
<input type="checkbox"/>	Computer security files – with personal information in the database, collected in order to grant user IDs

	Other (specify):
	Comment:

Other lines of business (specify uses):

X	CTS is a Correspondence Tracking System and FMS2 is a tool used to process FOIAs. It collects personal name and address of the writer from the incoming request to be able to respond to the correspondence via system-generated emails or generated MS Word documents. The system provides access permissions to restrict access if the subject so requires. It will be used to track correspondence and respond to correspondence from the public.

Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module 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?
	HUD module/application? (specify the module(s)/application(s) name)
	Others? (specify):
X	Comment: N/A

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
X	Comment: We only collect enough information to allow HUD to respond to letters or enquiries to the agency

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 Users must use a high strength password.
X	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated? <p>The CTS Team has notified CTS Users and user management that the CTS system administrator should be notified when users change job positions, are terminated, or no longer need access to system. When people leave HUD, a HUDgone is supposed to be filed that will remove their access to the HUD LAN and Intranet. Otherwise, users are automatically deactivated after 90 days of inactivity or 1 day after the system administrator has been notified by the user’s management to terminate system access.</p> <ul style="list-style-type: none"> • How do you know that the former employee no longer has access to your system? <p>Users who no longer have access to the HUD intranet, cannot access CTS. CTS uses HUD’s Active Directory for login and password information. When a user leaves HUD, part of the out processing procedures inactivates the user ID in Active Directory.</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"> • Full access rights to all data in the system: Approximately four (2) Application System Administrators Limited/restricted access rights to only selected data: The other 500+ users have limited or restricted access based on user group.
X	<p>Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? Instructions will be provided to those HUD individuals receiving correspondence requests as to requirements for safeguarding those copies.</p>
	<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</p>

	resides in another? Explain the existing privacy protections, or your plans to improve: CTS and FMS2 is a standalone system and does not share files or databases with other internal systems.
	Other methods of protecting privacy (specify):
	Comment:
Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated.	
We are currently identifying and documenting the risks and mitigation strategy for maintaining the data.	

Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

<input checked="" type="checkbox"/>	Name: Requestor Name
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
<input checked="" type="checkbox"/>	Personal e-mail address
	Other (specify):
	None
	Comment:

Question 8: What type of Notice(s) are provided to the individual on the scope of information collected, the opportunity to consent to uses of said information, the opportunity to decline to provide information.

- a. Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on form(s), and/or a system of records notice published in the Federal Register.) If notice was not published, why not?

Currently, there is no privacy notice in the system.

b. Do individuals have an opportunity and/or right to decline to provide information?

The person requesting the information must provide the information required to receive the correspondence.

c. Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent? No, information will only be used to return the correspondence requested.

Question 9: What are the Retention Use and Disposal Practices. Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.

a. How long is information retained?

The data will be maintained according to HUD's handbook for Retention Use & Disposition Schedule.

b. Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The disposition schedule is currently being finalized with the NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

We are currently identifying and documenting the risks and mitigation strategy for maintaining data according to the disposition schedule.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER