

U.S. Department of Housing and Urban Development

Office of Single Family Housing

RightNow CRM System (P256)

Privacy Impact Assessment

May 13, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **RightNow**. 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/ Belinda Martin](#)

**BELINDA MARTIN, MANAGEMENT ANALYST,
DAS, OFFICE FOR SINGLE FAMILY HOUSING
- SYSTEM OWNER**

[5/28/08](#)

Date

[/s/ Phillip Murray](#)

**PHILLIP A. MURRAY, ACTING DAS FOR
SINGLE FAMILY HOUSING**

[5/28/08](#)

Date

[N/A](#)

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

Date

[/s/ Donna Robinson-Staton](#)

**DONNA ROBINSON-STATON,
DEPARTMENTAL PRIVACY ACT OFFICER**
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

[6/5/08](#)

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT	7
Question 1: Provide a brief description of what personal information is collected.....	7
Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?	8
Question 3: Type of electronic system or information collection.....	9
Question 4: Why is the personally identifiable information being collected? How will it be used?	10
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	11
Question 6: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?	12
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	13
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	15
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	16

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

RightNow CRM System

(for IT Systems: Insert N/A, and Insert PCAS # Non-WCF Project)

May 13, 2008

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 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 Single Family Housing

Subject matter expert in the program area: Belinda Martin, Management Analyst, DAS, Office for Single Family Housing, Department of Housing and Urban Development, (202) 708-3175

Program Area Manager: Phillip A. Murray, Acting DAS for Single Family Housing, Department of Housing and Urban Development, (202) 708-3175

IT Project Leader: Paul E. Theisen, Director of Real Estate Insurance Division, Office of the Chief Information Officer, Office of Systems Integration and Efficiency, (202) 708-1587

For IT Systems:

- **Name of system:** RightNow CRM System
- **PCAS #:** No-WCF Project
- **OMB Unique Project Identifier #:** N/A
- **System Code:** P256

For Information Collection Requests:

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

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

The RightNow Technology Database collects contact related information to support answering the public regarding home ownership. The database is owned by the CMC who provides guidance and assistance to the public, and to several specific industry groups, concerning all aspects of the Federal Housing Administration's (FHA) mortgage insurance process. The minimal PIA collected is primarily used to create an interaction history between the caller and the Single Family Housing Program. The PII may be used to identify areas of improvement for the caller interaction, marketing and program development. The CMC serves as the single point of entry for consumers and lending institution experts.

Public and housing industry inquiries total one million contacts per year. Single Family has restructured its client management operation into a single Client Management Center, servicing all client types (public and lender) and communication channels (phone, email, fax). The CMC also maintains a comprehensive knowledgebase of Single Family policies and procedures and integrates with SFISnet, a portal to real-time FHA case data.

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
	Social Security Number (SSN)
	Other identification number (specify type):
	Birth date
X	Home address
X	Home telephone number
X	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
X	Comment: System collections other information such as the client/ industry type, business focus and responsibilities. The client has the authority to decline providing any of the information collected.

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):
X	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)?		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?		

Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbucks) or is remote access permitted from all areas outside the Department? Remote access is restricted.
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)?
Comment:

Question 3: Type of electronic system or information collection.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes	No
If yes, please proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Does the system require authentication?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)? Yes, external facing. No external users are not required to authenticate. Only The First Client (TFC) and HUD employees have access to the data, the public does not have any access to the data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

B If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

N/A	Conversion: When paper-based records that contain personal information are converted to an electronic system
N/A	From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
N/A	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
N/A	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
N/A	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)

N/A	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
N/A	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
N/A	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
N/A	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

C. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.

	Yes, this is a new ICR and the data will be automated
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	Comment:

Question 4: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

	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
X	Other (specify): To link past interactions with the Client Management Center (CMC)/FHA Single Family Program with current/real time caller interaction received from the public and housing industries. .
	Comment:

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):
	Comment:

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):
	Comment:

Fair Housing:

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

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):
	Comment:

Other lines of business (specify uses):

Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government?)

Only information disclosed is that in response to a subpoena or order issued by a U.S.-based court as specified below. Otherwise, no information is disclosed outside the agency.

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	<p>Comment: In accordance with Title 5 U.S.C. Section 552a (b), CMC is permitted to release customer information in response to a subpoena or order issued by a U.S.-based court. We are further permitted to release information to other government organizations to enable them to perform their official duties. These other government organizations are:</p> <ul style="list-style-type: none"> • law enforcement agencies on the federal, state or local level; • employees or representatives of the General Accounting Office (GAO); and • members of Congress, or their authorized representatives. <p>• a government organization requesting access to customer information must:</p> <ul style="list-style-type: none"> • submit the request in writing to the HUD program official; • identify the specific information needed; and • specify the official nature of the request (such as a criminal investigation, audit, etc.). <p>The HUD-CMC program official determines whether the organization’s need for the information is justified, and responds to the request based on that determination.</p>

Question 6: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

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
	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): The CMC collects PII only for the purposes of matching past records with current/real time interaction with the caller so that a “history” exists for that caller. If the caller does not want to provide PIA then the CMC will still respond to the caller’s question concerning FHA and will not include PIA information in the recorded incident.

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	<p>When an employee leaves:</p> <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? One Day • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): The termination process is as follows: Manager will find cause for termination, will terminate and will collect all company property, including card access to the facility. The manager notifies the IT/Security personnel who maintain all employees' access to all systems. The CMC IT/Security personnel will monitor the removal access for all these systems using a checklist.
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: 3 HUD HQ FHA Single Family employees have full access rights. • Limited/restricted access rights to only selected date: 3 HUD HQ FHA Single Family employees/Field Office Staff, plus 550 CMC employees <p>Access to system information is selectively granted based on the employee's need to perform his/her official duties. When an employee's or contractors duties change, then his/her access rights are changed accordingly or withdrawn entirely.</p> <p>To maintain the integrity of the system and its data CMC employees receive training to further improve their handling of sensitive information and understanding of security issues. All CMC users receive regularly scheduled security awareness refresher training, which is required by CMC policy.</p> <p>System users are trained in the security controls of the system, including rules of behavior and the consequences of violating the rules. CMC also provides to our employees regularly updated instructional material (both printed and posted on our Intranet website) on security issues.</p> <p>To further ensure that employees limit their access to customer information to legitimate and authorized business uses, the system uses logical access controls to regulate user behavior. Logical access controls are the system-based mechanisms used to specify which individuals and/or processes are to have access to a specific system resource, and the type of access that is to be permitted. These controls limit users' access to information and restrict their access on the system to their designated level.</p>

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): There are no discs, tapes or paper in use by RightNow. Data is stored on servers in the RightNow locations. The server is in a room that contains a combination lock at the point of entry with limited and monitored access to the facility.
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: RightNow is not integrated with any HUD systems and therefore no data is transferred to other systems.
	Other methods of protecting privacy (specify):
	<p>Comment: In accordance with Title 5 U.S.C. Section 552a (b) (1) and (2), CMC controls employee access to bondholder information. Confirmed</p> <p>The information utilized by CMC is categorized as Sensitive But Unclassified (SBU), however only properly authorized users have access to the information. HUD has implemented suitable system, personnel and physical security measures to adequately protect the integrity and security of this information.</p> <p>System Security Measures: CMC meets the specific security requirements established by the Federal Information Security Management Act (FISMA), OMB Circular A-130 and guidance from the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST). The system was certified to be compliant with these provisions as a result of an OMB A-130 Certification and Accreditation (C&A) security review in May 2006. On May 19, 2006, the Authorizing Official for the system certified that the system is compliant with the federal standards cited above and is authorized to continue operations. This accreditation is valid through May 2009.</p> <p>In addition to periodic C&A security reviews, CMC maintains the controls to ensure that continuous monitoring of the system is performed. Continuous monitoring consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. These activities are performed continuously throughout the life cycle of the system.</p> <p>CMC has a multiple automated system edits and input controls to prevent users from initiating erroneous and/or unauthorized transactions. New edits introduced to the system and existing edits are thoroughly tested prior to deployment. Management controls supplement logical and physical protections by requiring regular and frequent review of audit trails, audit logs, and access violation reports. CMC's computing infrastructure is subject to frequent independent audits and</p>

	<p>regular security reviews.</p> <p>Personnel Security Measures: CMC has implemented a detailed security infrastructure to ensure that all employees have been screened and can be afforded a level of trust commensurate with the duties of the individual. These measures comply with the Office of Personnel Management (OPM) human resource guidelines. Background investigations (in accordance with Executive Orders 12958 and 12968; OMB Circular No. A-130; and Title 5 of the Code of Federal Regulations sections 731,732, and 736) are conducted on all newly hired CMC employees. Regular background reinvestigations are conducted on existing employees as a condition of continued employment. These reinvestigations are conducted approximately every five years. All positions have been reviewed to ensure they have been classified at the proper sensitivity level during these investigations and reinvestigations.</p> <p>Physical Security Measures: Physical security at CMC buildings consists of entering the proper key code and possession of the proper CMC credentials. Walk-through and hand-held metal detectors are not required. Entry to the buildings is only permitted to individuals authorized by the CMC Project Manager (PM). The PM issues ID cards, which are validated upon completion of initial employee training, and recovered upon separation. This measure prevents unauthorized persons from gaining entry by using a lost or stolen ID card. All interior doors are equipped with dual combination key and cipher locks, which have been guaranteed by the manufacturer to be unique in the area.</p>

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

Mark any that apply

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

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

The RightNow system is not a potential privacy risk. The system collects a limited amount of personal information; it is password protected and only users with a need-to-know are authorized to access data within RightNow. Additionally, there are adequate administrative controls and security measures in place to ensure protection of this data. Please refer to “question 6” for details on this information.