

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

---

**Office of the Chief Procurement Officer  
(OCPO)**

**HUD Integrated Acquisition Management System  
(HIAMS)**

Privacy Impact Assessment

**September 27, 2011**

## DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for HUD Integrated Management 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.

### 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/ Elie Stowe](#)

\_\_\_\_\_  
**System Owner**

Elie Stowe

Office of the Chief Procurement Officer

[9/30/11](#)

\_\_\_\_\_  
**Date**

[/s/ Kenya Theus](#)

\_\_\_\_\_  
**Program Area Manager**

Kenya Theus

Office of the Chief Procurement Officer

[9/28/11](#)

\_\_\_\_\_  
**Date**

[/s/ Harlod Williams for Donna Robinson-Staton](#)

\_\_\_\_\_  
**Departmental Privacy Act Officer**

Donna Robinson-Staton

Office of the Chief Information Officer

U. S. Department of Housing and Urban Development

[9/30/11](#)

\_\_\_\_\_  
**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 general description of the system that describes:.....	7
Question 2: Type of electronic system or information collection.....	9
Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?.....	11
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)?.....	12
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)?.....	13
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?.....	14
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. ....	15
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.....	15
<b>SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....</b>	<b>17</b>
<b>APPENDIX A, CCR USER’S GUIDE.....</b>	<b>18</b>

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
PRIVACY IMPACT ASSESSMENT (PIA) FOR:  
HUD INTEGRATED ACQUISITION MANAGEMENT SYSTEM**

**for IT System: OMB Unique Project Identifier #: 025-00-01-05-01-1050-00  
and CSAM#: P263**

**3/11/2011**

**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](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](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](#) (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>); 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 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 the Chief Procurement Officer (OCPO)*

**Subject Matter Expert in the Program Area:** *Keith Surber*

**Program Area Manager:** *Kenya Theus*

**IT Project Leader:** *Angela Campbell*

### For IT Systems:

- **Name of system:** *HUD Integrated Acquisitions Management System (HIAMS)*
- **PCAS #:** *00663600*
- **OMB Unique Project Identifier #:** *025-00-01-05-01-1050-00*
- **System Code:** *P273*
- **Development Date:** *September 2010-October 2011*
- **Expected Production Date:** *October 15<sup>th</sup> 2011*

### For Information Collection Requests:

- **Name of Information Collection Request:** *N/A: There is no ICR*
- **OMB Control #:** *N/A*

### 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?** (e.g. name, address, gender/sex, race/ethnicity, income/financial data, employment history, medical history, Social Security Number, Tax Identification Number, Employee Identification Number, FHA Case Number)

*HIAMS will collect and store Vendor Tax ID Numbers (TIN). The situation where this becomes PII data is when a small business uses an individual's social security number (SSN) as its Tax ID Number.*

*As mitigation, when small business owner's SSN is used as their TIN, there is no differentiation between the two. The SSN will be presented to the users within HIAMS as the TIN so they will appear the same. In addition, the TIN is stored in the HIAMS vendor profile; access to the vendor profile is limited to authorized users -- the Contracting Officer, the Buyer and the HIAMS System Administrator.*

- b. **From whom is the information collected (i.e., government employees, contractors, or consultants)?**

*The tax ID number is collected from the vendor via Central Contractor Registry (CCR). CCR is the source of the data for HIAMS.*

**c. What is the functionality of the system and the purpose that the records and/or system serve?**

- *The Office of the Chief Procurement Officer (OCPO) is implementing the HUD Integrated Acquisition Management System (HIAMS) as an enterprise wide, end-to-end acquisition management solution. The records maintained in the system include acquisition or procurement related data from planning through contract completion. As defined by NIST SP 800-60, the data types contained in HIAMS are:*
  - *Budget Execution Information is required in the system to facilitate the financial transactions throughout the procurement process. Budget Execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses.*
  - *Goods Acquisition Information which involves the procurement of physical goods, products, and capital assets to be used by the Federal government.*
  - *Services Acquisition Information involves the oversight and/or management of contractors and service providers from the private sector.*
- *The Tax ID number is used as the vendor identifier for the financial system.*
- *CO's and Buyers use the TIN to verify that the selected vendor is the one they intend to work with.*
- *Non-buyers do not have the ability to view vendor profiles in HIAMS. In order for the Government Technical Representative (GTR. ) to be able to manually verify vendors with the Financial System, the TIN will be printed on award documents. The award documents will also have limited distribution to the Contracting Officer (CO)/Contracting Specialist (CS), GTR, Government Technical Monitor (GTM), the CFO office or appropriate payment office, and the Small Business Administration for 8(a) awards.*
- *If the award form is requested outside of HUD via a FOIA the TIN is redacted.*

**d. How is information transmitted to and from the system?**

*Information is either manually input by a government employee or uploaded into HIAMS from one of the Integrated Acquisition Environment (IAE) systems, the HUD financial system, or the FedConnect Vendor Portal. SSL is used to transmit data to and from any external system (IAE or FedConnect). Oracle BPEL (Middleware) connects all internal systems.*

**e. What are the interconnections with other systems?**

*HIAMS will interconnect with the following external system: Central Contractor Registration, Federal Procurement Data System - Next Generation (FPDS-NG), Online Representations and Certifications Application (ORCA), FedBizOps, and FedConnect, and internally with HUDCAPS and its Financial DataMart (FDM). Initially, a custom integration will be developed with HUDCAPS Financial system. In the future with the new PeopleSoft HUD Integrated Core Financial System (HICFS) once it's deployed.*

**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)?**

*According to the Federal Acquisition Regulation (FAR) policy FAR 4.1102 (November 1, 2003), Prospective contractors shall be registered in the CCR database prior to award of a contract or agreement. Federal Acquisition Circular (FAC) 2001-16 amends the FAR policy to require contractor Registration in the CCR database effective November 1, 2003.*

*HIAMS relies on CCR to provide system use notification regarding use of data passed from CCR to HIAMS. Prior to registering with CCR, potential users are told in the CCR Users Guide that their TIN is required to register and this information is essential for government contracting. It is clearly stated that the information can be used by other government systems. The privacy policy is also available to all who access CCR. (You can Click [Here](#) for a direct link to the CCR Users Guide) The user's guide and privacy policy is also attached as Appendix A.*

**Question 2: Type of electronic system or information collection.**

	Yes	No
<b>A. If a new electronic system (or one in development)</b> (implemented after April 2003, the effective date of the E-Government Act of 2002)?	<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)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

<b>B. If this is existing electronic system has the system undergone any changes (since April 17, 2003)? If an existing system, when was the system developed? <u>N/A</u></b>	<b>Yes</b> <input type="checkbox"/>	<b>No</b> <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 type="checkbox"/>
If yes, please explain:		

<b>C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred:</b> 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):	
<input checked="" type="checkbox"/>	<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)

<b>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?</b> 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.	
	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u> )
	Comment: <i>This is not applicable; there are no ICRs.</i>

**Question 3: Explain by Line of Business why 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):
	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: See internal operations

**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):**

X	<b>Acquisition Management:</b> Procurement of goods and services. Information required 1) for interface with financial system for funds commitment and obligation; and 2) to provide a mechanism for vendor verification for award and payment.
	<b>Comment:</b> The TIN number collected by CCR and transmitted to HIAMS may be the social security number with some small business owners.

**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?
X	<b>HUD module/application?</b> HIAMS and HUD's financial system use the TIN as the vendor identifier.
	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: <b>CCR requirement</b>

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:

<input checked="" type="checkbox"/>	System users must log-in with a password (Please specify password type): Integrated with Active Directory.
<input checked="" type="checkbox"/>	When an employee leaves: <ul style="list-style-type: none"> <li>• How soon is the user ID terminated? <i>A user ID is inactivated on the date of their termination as specified by the HUD 58.</i></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): <i>The ISSO receives a notice the employee has is no longer with HUD and ensures that the HIAMS account is inactivated. The user will also have been inactivated from Active Directory by the security officer, so they will no longer be able to access the network.</i></li> </ul>
<input checked="" type="checkbox"/>	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: Full access rights to all data in the system: <i>Approximately two (2) Application System Administrators</i> Limited/restricted access rights to only selected data (TIN included in this data): <i>Approximately one (1) Site Administrator per site: seven (7) total</i> <i>Approximately one (1) Buyer per site: seven (7) total</i> <i>Approximately one (1) Contracting Officer per site: seven (7) total</i>  <i>This access is defined by the security group configuration.</i>  Total number of authorized users will be approximately 23-30
<input checked="" type="checkbox"/>	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):

	<i>Instructions will be provided to those HUD individuals receiving Award copies as to requirements for safeguarding those copies.</i>
<input checked="" type="checkbox"/>	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: <i>The TIN number is used to identify vendors in the financial system, HUDCAPS, and is stored in the Datamart. Data protection within Datamart and HUDCAPS is managed by the HUD CFO Office and their contractor support services.</i>
	Other methods of protecting privacy (specify):
	Comment:
<p><b>Privacy Impact Analysis:</b> Given the access and security controls, what privacy risks were identified and describe how they were mitigated.</p> <p><i>Within HIAMS, the TIN is restricted on a need to know basis based on duties. It can only be viewed by Contracting Officers, Buyers, System Administrators, and Site Administrators from the vendor profile page. It cannot be changed.</i></p> <p><i>The TIN is displayed and printed on the award document. This risk is mitigated by limiting access to authorized HUD personnel only and by providing instructions on handling the sensitive data. If the document is FOIA'D, the TIN is redacted.</i></p>	

**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: Vendor Name
	Social Security Number (SSN)
<input checked="" type="checkbox"/>	Identification number (specify type): DUNS Number
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	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?**

*Prior to registering with CCR, potential users are told in the CCR Users Guide that their TIN is required to register and this information is essential for government contracting. It is clearly stated that the information can be used by other government systems. The privacy policy is also available to all who access CCR. (You can Click [Here](#) for a direct link to the CCR Users Guide) The user's guide and privacy policy is also attached as Appendix A.*

*The CCR and HIAMS network and application banner provide notice of the use of Privacy data.*

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

*This opportunity is provided when choosing whether or not to register for CCR.*

- 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?**

*By choosing to register for CCR, contractors are consenting to the use of their TINs for contracting, tracking, and auditing purposes. Businesses and other organizations are required to register in CCR in order to do business with the Federal Government.*

**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?**

*Record retention and disposal are in accordance with FAR subpart 4.7 for Contractor Records Retention. HIAMS has the ability to store archived data and is defaulted at seven years. This complies with all federal regulations.*

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

*This is not applicable. HIAMS stores electronic records and NARA is not yet storing electronic records for HUD.*

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

*There is no additional risk associated. It is retained in the archive database and has the same protection as all other procurement data.*

**SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER**

## APPENDIX A, CCR USER'S GUIDE

### Central Contractor Registration (CCR) Policy

- According to the [FAR 4.11](#), prospective vendors must be registered in CCR prior to the award of a contract; basic agreement, basic ordering agreement, or blanket purchase agreement.
- According to [FAR 52.204-7](#), to register in CCR, a firm must have a Data Universal Numbering System (DUNS) number. The DUNS Number is assigned by Dun & Bradstreet, Inc. (D&B) to identify unique business entities.

EFT and assignment of claims as stated [FAR 52.232-33](#) Para. G.: "EFT and assignment of claims. If the Contractor assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Contractor shall require as a condition of any such assignment, that the assignee shall register in the CCR database and shall be paid by EFT in accordance with the terms of this clause. In all respects, the requirements of this clause shall apply to the assignee as if it were the Contractor. EFT information that shows the ultimate recipient of the transfer to be other than the Contractor, in the absence of a proper assignment of claims acceptable to the Government, is incorrect EFT information within the meaning of paragraph (d) of this clause."

### Federal Agency Registration (FedReg) Policy

- [OMB Memorandum M-03-01](#) and the Treasury Financial Manual Bulletin No. 2007-03, [Intergovernmental Business Rules](#), require all federal agencies that engage in buying or selling goods/services to other federal agencies to register in the Federal Agency Registration database (FedReg).
- At a minimum, this registration must be at the major component level. Registration at the major component level will assist agencies in identifying intragovernmental transactions below the Department level.

In the near future, the registration data will be used to route intragovernmental transactions electronically through the Intragovernmental Transaction Portal (IGTP), currently being tested, and to facilitate automated settlement through Treasury's IPAC system.

### Exceptions to the CCR registration requirement

The FAR policy requiring registration in CCR applies to all types of awards except the following:

- Purchases that use a Government wide commercial purchase card as both the purchasing and payment mechanism, as opposed to using the purchase card only as a payment method;
- Classified contracts (see 2.101) when registration in the CCR database, or use of CCR data, could compromise the safeguarding of classified information or national security;
- Contracts awarded by-
  - Deployed contracting officers in the course of military operations, including, but not limited to, contingency operations as defined in 10 U.S.C. 101(a)(13) or humanitarian or peacekeeping operations as defined in 10 U.S.C. 2302(7); or
  - Contracting officers in the conduct of emergency operations, such as responses to natural or environmental disasters or national or civil emergencies, e.g., Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121);
- Contracts to support unusual or compelling needs (see 6.302-2);
- Awards made to foreign vendors for work performed outside the United States, if it is impractical to obtain CCR registration; and
- Micro-purchases that do not use the electronic funds transfer (EFT) method for payment and are not required to be reported (see Subpart 4.6).

Please note that any information provided in your registration may be shared with authorized federal government offices. However, registration does not guarantee business with the federal government.

## Background

Central Contractor Registration (CCR) is the primary registrant database for the U.S. Federal Government. CCR collects, validates, stores, and disseminates data in support of agency acquisition missions, including Federal agency contract and assistance awards. Please note that the term "assistance awards" includes grants, cooperative agreements and other forms of federal assistance. Whether applying for assistance awards, contracts, or other business opportunities, all entities are considered "registrants".

Both current and potential federal government registrants are required to register in CCR in order to be awarded contracts by the federal government. Registrants are required to complete a one-time registration to provide basic information relevant to procurement and financial transactions. Registrants must update or renew their registration at least once per year to maintain an active status. In addition, entities (private non-profits, educational organizations, state and regional agencies, etc.) that apply for assistance awards from the Federal Government through Grants.gov must now register with CCR as well. However, registration in no way guarantees that a contract or assistance award will be awarded.

CCR validates the registrant information and electronically shares the secure and encrypted data with the federal agencies' finance offices to facilitate paperless payments through electronic funds transfer (EFT). Additionally, CCR shares the data with federal government procurement and electronic business systems.

## Grants Policy

Grants.gov was born as a governmental resource named the E-Grants Initiative, part of the President's 2002 Fiscal Year Management Agenda to improve government services to the public:

"Agencies will allow applicants for Federal Grants to apply for and ultimately manage grant funds online through a common web site, simplifying grants management and eliminating redundancies."

The concept has its origins in the Federal Financial Assistance Management Improvement Act of 1999, also known as [Public Law 106-107](#). P.L. 106-107 was enacted in November of that year and the purposes are to:

1. Improve the effectiveness and performance of Federal financial assistance programs.
2. Simplify Federal assistance application and reporting requirements.
3. Improve the delivery of services to the public.
4. Facilitate greater coordination among those responsible for delivering the services.

The 26 Federal agencies that award grants and cooperative agreements are actively implementing P.L. 106-107 through interagency work groups, developing common data elements, electronic processes and uniform administrative rules across agencies.

## Central Contractor Registration Privacy and Security Statement

\*\*\*\*\*WARNING\*\*\*\*\*

This is a U.S. Federal Government computer system

"FOR OFFICIAL USE ONLY"

This system is subject to monitoring. Therefore, you can assume no expectation of privacy. Unauthorized activities are subject to disciplinary action including criminal prosecution. Furthermore, you expressly consent to our use of cookies and clear GIFs (Graphic Interchange Format files) when you use our services.

\*\*\*\*\*WARNING\*\*\*\*\*

Thank you for visiting the Central Contractor Registration (CCR) website and reviewing the following privacy and security statement.

The CCR Website is part of the Integrated Acquisition Environment, one of the EGovernment initiatives in the President's Management Agenda.

We are strongly committed to maintaining the privacy of your personal information and the security of CCR computer systems. With respect to the collection, use and disclosure of personal information, the agencies involved in the development of CCR make every effort to ensure compliance with applicable Federal law, including, but not limited to, The Privacy Act of 1974, The Paperwork Reduction Act of 1995, and The Freedom of Information Act. Collection of that information is authorized by Defense Federal Acquisition Regulation, 48 C.F.R. Subpart 204.7302; Debt Collection Improvement Act of 1996, Public Law 104-134; Government Streamlining Act of 1994, Public Law 103-355.

The principal purpose for collecting data is to have a primary database for current, accurate, and complete Federal contractor and grantee registrant information. The CCR provides a central database and application suite that records, validates, and distributes specific data about government and commercial trading partners. CCR validates registrants' information and electronically shares it—as secure encrypted data—with appropriate federal agencies' finance offices to facilitate electronic funds transfer (EFT) payments. CCR shares that data with federal government procurement and electronic business systems. The CCR is not designed to collect personally identifying information from individuals who are not acting in their entrepreneurial capacities. Click [here](#) to see the data elements and descriptions of the information collected via CCR registration. The CCR Public Search allows the viewing of public information about CCR registrants. Private information is restricted to authorized government officials. Registrant provided contact information, including email addresses and company address information, may be used to forward items of interest.