U.S. Department of Housing and Urban Development

Office of Native American Programs

ONAP Training and Technical Assistance Notice of Funding Availability Information Collection

Privacy Impact Assessment

August 23, 2012

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **ONAP Training and Technical Assistance NOFA Information Collection**. 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.

SYSTEM OWNER	**Date**

Rodger Boyd, Deputy Assistant Secretary
Office of Native American Programs
HUD (Room 4126)
451 7th Street
Washington, DC 20410
202-402-3326
rodger.j.boyd@hud.gov

PROGRAM AREA MANAGER	**Date**

Mike Andrews, Director
Headquarters Operations
Office of Native American Programs
HUD (Room 4126)
451 7th Street
Washington, DC 20410
202-402-6329
mike.andrews@hud.gov

DEPARTMENTAL PRIVACY ACT OFFICER	**Date**

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

TABLE OF CONTENTS

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

ONAP TRAINING AND TECHNICAL ASSITANCE NOTICE OF FUNDING AVAILABILITY INFORMATION COLLECTION

August 23, 2012

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 Handbook1325.1 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 superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security

regulations at Title 44 U.S. Code chapter 35 subchapter II
(http://uscode.house.gov/search/criteria.php); and
- OMB Circular A-130, Management of Federal Information Resources, Appendix I
(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).

5

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 <u>new</u> collection and <u>automated</u>, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The [Privacy Act of 1974](#), as amended (http://www.usdoj.gov/foia/privstat.htm) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The [E-Government Act of 2002](#) requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is 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 Native American Programs
Subject Matter Expert in the Program Area: Mike Andrews
Program Area Manager: Mike Andrews
IT Project Leader: N/A

For IT Systems: N/A
- **Name of system:**
- **PCAS #:**
- **OMB Unique Project Identifier #:**
- **System Code:**
- **Development Date:**
- **Expected Production Date:**

For Information Collection Requests:
- **Name of Information Collection Request: ONAP Training and Technical Assistance Notice of Funding Availability Information Collection**
- **OMB Control #: Information collection currently under OMB review**

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)
>
> Name, Address, and Employer Identification Number
>
> b. **From whom is the information collected (i.e., government employees, contractors, or consultants)?**
>
> Nonprofit and for-profit entities
>
> c. **What is the functionality of the system and the purpose that the records and/or system serve?**
>
> Entities will respond to a Notice of Funding Availability (NOFA) to deliver training and technical assistance services on behalf of the Office of Native American

Programs (ONAP) and for the benefit of recipients of Indian Housing Block Grants and Native Hawaiian Housing Block Grants. Response to the NOFA is voluntary. ONAP will review all proposals submitted to www.Grants.gov and award cooperative agreements to the most qualified entities.

d.   How information is transmitted to and from the system;

Responses to the NOFA are required to be submitted electronically to the federal-wide Grants.gov system. ONAP will receive copies of all proposals submitted to the website, rate and rank the proposals, and enter into cooperative agreements.

e   What are the interconnections with other systems.

Applications submitted to Grants.gov are forwarded to HUD's Grant Interface Management System (GIMS II: PCAS 252200) which is a central repository for collection of all electronic applications for competitive funding. ONAP will rely on HUD's Line of Credit Control System to receive invoices from and make payments to the awardees.

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 forms associated with the NOFA are HUD forms that have been approved by OMB.

Question 2: Type of electronic system or information collection.

	Yes	No
A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	☐	☐
Does the system require authentication?	☐	☐
Is the system browser-based?	☐	☐
Is the system external-facing (with external users that require authentication)?	☐	☐

	Yes	No
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? Grants.gov was developed by OMB in FY 2006. GIMS II was developed in FY 2007 and is owned by OSPM. GIMS II is updated periodically to meet new technology requirements and Grants.gov requirements.	X ☐	☐

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?	☐	X ☐
If yes, please explain:		

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):

	Conversion: When paper-based records that contain personal information are converted to an electronic system
	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
	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)
	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)
	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)
	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)
	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	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)

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.

X	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: Responses to the NOFA will be submitted to Grants.gov and transferred to HUD's GIMS II.

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:

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	Cooperative Agreements for delivery of training and technical assistance services to federally-recognized tribes and tribally designated housing entities.
	The personally identified information is collected to verify the identity, qualifications, and capabilities of non-profit and for-profit corporations responding to the NOFA. Successful respondents will enter into a Cooperative Agreements with HUD.

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):
	Comment: HUD will share only the name, address, and contact information of the awardees under the NOFA with interested parties, as authorized by law and as necessary to carry out agency responsibilities.

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
	Comment: The NOFA is collecting personal information on OMB-approved forms that HUD requires in its standard NOFAs.

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 (Please specify password type) Grants.gov registration is required.
	When an employee leaves: • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve):
	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: Limited/restricted access rights to only selected data:
	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):
	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:
	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. No known privacy risks are associated with Grants.gov or with HUD's record keeping system.	

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

Mark any that apply

X	Name:
	Social Security Number (SSN)
X	Identification number (specify type): Employer Identification 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?

Yes. On March 20, 2012, the Federal Register published the 60-day comment notice of the information collection associated with the NOFA. On May 30, 2012, the Federal Register published a 30-day comment notice of the information collection associated with the NOFA. See attached notices.

  b. Do individuals have an opportunity and/or right to decline to provide information?
Response to the NOFA is voluntary; however, applicants are required to provide personal information when completing OMB-approved forms that are standard with HUD NOFAs.

  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.

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?**
For the records under its control, ONAP will comply with HUD's record retention and disposal policies.

b. **Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?**
ONAP assumes that HUD's record retention schedule has been approved by the component officer and NARA.

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

There are no known risks associated with HUD's record retention requirements.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER