

U.S. Department of Housing and Urban Development

Public and Indian Housing

Tracking-at-a-Glance[®] (TAAG)
(Case Management System for the Disaster Housing
Assistance Program (DHAP))

Privacy Impact Assessment

May 30, 2008

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **Tracking-at-Glance**. 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/ TONY HEBERT

TONY HEBERT, SYSTEM OWNER
PIH Urban Revitalization Division
Resident Supportive Services

6/5/08

Date

/S/ RON ASHFORD

RON ASHFORD, PROGRAM AREA MANAGER
PIH Urban Revitalization Division
Resident Supportive Services

6/30/08

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

7/7/08

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT	7
Question 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? If yes, what security controls are in place to protect the information e.g., encryptions (give details below)?	9
Question 3: Type of electronic system or information collection.....	11
Question 4: Why is the personally identifiable information being collected? How will it be used?	12
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	14
Question 6: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use	14
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	15
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	16
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	16

FINAL/APPROVED

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT PRIVACY IMPACT ASSESSMENT (PIA) FOR: TRACKING-AT-A-GLANCE® (TAAG)

**OMB Unique Identifier for IT Systems: N/A
and PCAS #: N/A**

May 30, 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: Public and Indian Housing Resident Supportive Services

Subject matter expert in the program area: Tony Hebert, Public and Indian Housing, Urban Revitalization Division, Department of Housing and Urban Development, (202) 402-7387.

Program Area Manager: Ron Ashford, Director, Resident Supportive Services – HOPE VI Division, Department of Housing Development, (202) 402-4258

IT Project Leader: Tony Hebert (Program/contact information reflected above)

For IT Systems:

- **Name of system:** Tracking-at-a-Glance® (TAAG)
- **PCAS #:** N/A, this is not a OMB/Working Capital Fund (WCF) project
- **OMB Unique Project Identifier #:** N/A, this is not a OMB/WCF project
- **System Code:** TAAG

For Information Collection Requests:

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

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

In July 2007, HUD and FEMA executed an Interagency Agreement (IAA) under which HUD acts as the servicing agency for administering the Disaster Housing Assistance Program (DHAP) program. Pursuant to FEMA's grant authority, grants are provided to local PHAs to administer DHAP on behalf of FEMA. Under DHAP, public housing authorities (PHAs) will make rental assistance payments on behalf of eligible families to participating landlords for the duration of the program, ending on March 1, 2009. In order to prepare the family for this eventuality, FEMA requires that case management services be provided for the entire duration of DHAP. The objectives of these services are greater self-sufficiency and permanent housing status for participating individuals and families. This will include assisting program participants identify non-disaster supported housing solutions such as other affordable housing options that may be available for income eligible families. PHAs are required to report case management outputs and outcomes through TAAG, which is the DHAP case management reporting system for the duration of the program.

TAAG will contain identifying information about the program participants and their household members including: name, social security number, FEMA ID number of eligible head of household member, birth date, current telephone number and current address. In addition, the files contain sensitive information about education level, employment and training needs, elderly and disabled status, social service needs and service referrals. The client provides information regarding education level, employment and training, disability status and social service needs as information that the case manager may use to assess any barriers to permanent housing

attainment and/or increased self-sufficiency. The case manager uses this information in order to identify appropriate service referrals, to help prepare clients for the eventual end of the DHAP in March 2009.

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:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Social Security Number (SSN) .
<input checked="" type="checkbox"/>	Other identification number (specify type): Federal Emergency Management Agency ID
<input checked="" type="checkbox"/>	Birth date
<input checked="" type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
<input checked="" type="checkbox"/>	Comment: Personally identifiable information is initially provided by FEMA to HUD in order to facilitate the delivery of rental assistance as is provided through the Inter-Agency Agreement. Housing Authorities update this information in the Public and Indian Housing Information Center (PIC), which is a current and separate IT system. This information is then transmitted through secure systems to TAAG to provide periodic updates of all DHAP eligible households.

Personal/ Sensitive Information:

<input checked="" type="checkbox"/>	Race/ ethnicity
<input checked="" type="checkbox"/>	Gender/ sex
	Marital status
<input checked="" type="checkbox"/>	Spouse name
<input checked="" type="checkbox"/>	# of children
<input checked="" type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
<input checked="" type="checkbox"/>	Employment history:
<input checked="" type="checkbox"/>	Education level
	Medical history/ information
<input checked="" type="checkbox"/>	Disability
<input checked="" type="checkbox"/>	Criminal record
	Other (specify):
	None
<input checked="" type="checkbox"/>	Comment: TAAG captures pertinent data relating to family self-sufficiency, permanent housing status and service needs. TAAG supports DHAP grantees in their case management efforts, HUD staff in their program monitoring activities and providing required reports to FEMA in fulfillment of its responsibilities outlined within the IAA. The system was procured through contract number: C-DEN-02199.

The system allows DHAP grantees to implement and report case management services for FEMA’s DHAP program, for which HUD is the servicing agent. This system will assist with the implementation and administering of rental housing assistance and case management services to individuals and families whose residence have been rendered uninhabitable as a result of the disaster caused by Hurricanes Katrina and Rita.

The personal and sensitive information, listed above, is provided by the client to the case management in order to document recipient demographic information, but more expressly for the purpose of identifying community or social services that the client may need assistance accessing. If a “No Response” is given by the client, the case manager cannot assist with accessing social services within the community. However, this does not necessarily affect the receipt of rental assistance through the DHAP.

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed? If yes, what security controls are in place to protect the information e.g., encryptions (give details below)?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

What security controls are in place to protect the information (e.g., encryptions)?

The servers are protected from the outside world by blocking all the ports that are not used, for example on the web servers, only port 80 and 443 will be open to the outside world, every other port will be blocked, this minimizes attacks. The servers are also running kaspersky antivirus server edition, all of them. The web servers are also load balanced across 2 Riverstone/Lucent 8000 routers to make sure that if any of the servers goes down, or any of the routers go down the secondary router and server will continue to operate and take up the slack, when the primary is brought up again, the system automatically continues to load balance between them. The 8000 series routers are running redundant power supplies and redundant control modules and redundant flash cards, no single failure of either the control modules, the flash cards or a power supply will affect any single 8000. But on top of all that there are 2 of them running VRRP – virtual router redundancy protocol to redirect traffic if necessary. The database servers are not even visible from the outside world, they are on a private network ONLY visible to the 2 web servers. The 2 database servers are clustered and running SQL 2000 enterprise, once again if any of the database servers goes down the other one continues to operate until the primary is brought back up. Both Database servers are attached to Network appliance through gigabit Ethernet, they both access the network appliance simultaneously, network appliance device is running RAID DP, that means it is RAID 5 with hot spare and DOUBLE parity drives for redundancy, it also has redundant power supplies. Also to be noted is that ALL of the above servers are running RAID 5 on their drives. They are hooked up to a 3000VA Tripplite Online UPS and that is backup up by a 150KVA generator that kicks on within 10secs of an outage. The generator has 7 days run time on current fuel and we have fuel contracts with 2 separate suppliers, the cooling for the system is controlled by redundant 7 ton AC units running concurrently in the NOC. Once again if a single AC system goes down, the secondary takes up the slack. On top of all this redundancy we have spare of all the routers and switches in our facility. The facility is fed by several upstream providers and the fibers that deliver the carriers is also diverse in that it runs to 2 separate carriers , BellSouth and FPL, these circuit are running concurrently so even if all of BellSouth's network goes down we continue to use the power companies fiber to connect to our internet circuits and vice versa.

What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?

The Tracking At A Glance application operates on a web server and does not reside behind HUD's current systems nor behind HUD's firewall. Therefore, there is no VPN or Citrix interface required nor is there any functionality to interact with HUD's systems. The TAAG web application does make use of secured socket layer (SSL) and have secure certification authority that is registered.

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/Starbuck) or is remote access permitted from all areas outside the Department?

DHAP grantees and their agents are bound by the Privacy Act Guidelines as stated within published program guidelines (PIH 2008-1). Additionally, the access of DHAP grantees, or public housing authorities and their agents, is restricted to only the households served by the PHA, rather than the entire database – which reflects only the data they have entered into the system.

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)? **DHAP grantees and their agents are bound by the Privacy Act Guidelines as stated within published program guidelines (PIH 2008-1). Additionally, the access of DHAP grantees, or public housing authorities and their agents, is restricted to only the households served by the PHA, rather than the entire database – which reflects only the data they have entered into the system.**

Comment: **Records are maintained on a secure computer network protected by a firewall. Access to system is restricted to authorized users only, requires a user ID and is password protected.**

Question 3: Type of electronic system or information collection.

Fill out Section A, B, or C as applicable.

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

	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)? Members of the public are not granted access to TAAG data? The access of DHAP grantees, or public housing authorities and their agents, is restricted to only the households served by the PHA, rather than the entire database – which reflects only the data they have entered into the system.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

N/A	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.

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>)
X	Comment: Approval to gather this data was obtained as part of the Disaster Housing Assistance Program ICR, OMB approval 2577-0252. The ICR was obtained to cover the collection of all data elements within TAAG and all other collections required for the administration of DHAP as DHAP represents a new federal program. Therefore, no prior collection authority existed. Within the OMB submission, the fact that TAAG is an automated system was noted within the ICR submission.

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
	Other (specify):
	Comment:

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
X	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
X	Other (specify): Individuals who are covered by this system are individuals and families displaced by Hurricanes Katrina or Rita, who receive rental subsidy through the DHAP and agree to all program requirements including case management.
X	Comment: Households receiving rental assistance under DHAP are required by FEMA to participate in case management services. The TAAG system is used to provide case management and document household information. Most information is provided by the client and is not explicitly required as a condition of receiving rental assistance.

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)?

Mark any that apply:

X	Federal agencies? Federal Emergency Management Agency (FEMA)
X	State, local, or tribal governments?
X	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
X	Non-profits?
	Faith-based organizations?
	Builders/ developers?
X	Others? (specify):
X	Comment: HUD administers the DHAP through an IAA with FEMA. As is required by the IAA, HUD will provide regular reports to FEMA of program activities. Information from TAAG will be reported in the aggregate for this purpose. Other users of the data include PHAs who are the DHAP grantees responsible for providing case management services to families through their grant agreement. Many PHAs contract out this responsibility to local providers either through contracts of Memorandums of Understanding (MOUs), including non-profits, to perform case management service. As a result, much of the data is gathered and input by local non-profits or case management providers who represent users of the system.

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. 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): Personally identifiable information such as name, social security number, current address and FEMA ID is provided by FEMA to HUD for the purpose of identifying household eligibility. A client may not “opt-out” of this personally identifiable information, which is used to determine DHAP eligibility status. However, sensitive information such as disability status, criminal history, as well as medical and employment history is provided by the client to the case manager at the client’s discretion. To the extent that a client provides this information, the case manager can help access services within the local community including job training, job placement and disability resources. However, if a client is not interested in accessing services through case management and does not need them to achieve self-sufficiency, a “No Response” could be provided. This would not terminate their DHAP rental assistance as long as they are complying with other case management
---	--

	requirements such as periodic meetings to update information and ensure the family is making progress towards self-sufficiency as needed. While the client must actively participate in case management with the goal of achieving permanent housing by March 2009, to the extent that services are not sought, clients are not required to provide specific information.
	No, they can't "opt-out" – all personal information is required
X	Comment: Participants are required to participate in case management services in order to receive rental subsidy benefits under the DHAP. However, participants are not required to provide specific sensitive information.

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password users create individualized passwords. They are not automatically generated by the system.
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? 24 hours • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): After the PHA notifies that a case manager has been terminated, the userid is de-activated and the password is changed to ensure that access will not be granted to the system.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system: There are only three users with "corporate" or full access rights to the system: two headquarters staff and the Technical Assistance provider team lead. • Limited/restricted access rights to only selected data: 1,526 as of 5/27/08
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): <p>Records are maintained on a secure computer network protected by a firewall. Access to system is restricted to authorized users only, requires a user ID and is password protected. No manual files with unique identifier information that would allow an individual to be linked to the information in the file will be maintained.</p> <p>Information is archived electronically and stored. Records will be retained and disposed of in accordance with the General Records Schedule included in HUD Handbook 2228.2, appendix 14, items 21-26.</p>
	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to

	improve: TAAG data are not transmitted, in any way, to another IT system.
	Other methods of protecting privacy (specify):
	Comment:

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: Public Housing Authority (PHA)/Participants
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
<input checked="" type="checkbox"/>	Other (specify): City/Zip code and general demographic characteristics
	None
	Comment: Users can perform a search function using the data elements identified above.

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

TAAG does require privacy protection since the system does collect and maintain personal/sensitive data about members of the public. Based on the Privacy Programs assessment of the PIA for TAAG we determined that there are adequate administrative controls in place to ensure the protection of this information.

Additionally, TAAG is classified as a Privacy Act System of Records (SOR); please refer to: http://www.hud.gov/offices/cio/privacy/documents/fed_reg_sornotice_taag.pdf to review the full text of the published SOR.