Privacy Impact Assessment Template

PLATEAU TALENT MANAGEMENT SYSTEM

This template is used when the Chief Privacy Officer determines that the system contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
Senior Agency Official for Privacy
Federal Housing Finance Agency
1700 G Street NW
Washington, DC 20552
(202) 414-3804
David.Lee@fhfa.gov

Guidance for completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form (IIF) is handled. PIAs are to be completed when FHFA: 1) develops or procures an IT system or project that collects, maintains, or disseminates IIF from or about members of the public; or 2) initiates a new electronic collection of IIF for 10 or more members of the public. PIAs are not required for collections of information from Federal employees. IIF about government personnel generally is protected by the Privacy Act; however the Office of Management and Budget (OMB) encourages agencies to conduct PIAs on these systems as appropriate. System owners and developers are responsible for completing the PIA. The guidance below has been provided to help system owners and developers complete a PIA.

Overview

- In this section, provide a thorough and clear overview of the system and give the reader the appropriate context to understand the responses. Some questions to consider include:
  - What is the purpose of the IT system?
  - What will be the primary uses of the system?
  - How will this support the program's mission?
- This section fulfills the E-Government Act's requirement for an introduction for members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

Section 1.0 Characterization of the Information

- Identify if the system contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.
- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider include:
  - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties. A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or an organization such as Neighborworks).
- If the system collects information from I 0 or more members of the public, ensure that the agency has received OMB prior approval to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the Office of General Counsel for assistance.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports the Agency's or Program's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).

- The retention periods of data/records that FHF A manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the system, the records schedules are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.
- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

Section 4.0 Notice, Access, Redress and Correction

- The Privacy Act requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. 552a(e)(l).
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the system retrieves information by an individual's name or other personal identifier (e.g. social security number) it is a Privacy Act system and may need a SORN published in the Federal Register. The system may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact the Privacy Act Officer. The Privacy Act requires that any amendments to an existing system must also be addressed in a Federal Register notice.
- If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.
- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (l 2 CFR Part l 204) that explains how individuals can gain access to information about themselves and correct errors, if appropriate.
- Any employee who knowingly and willfully maintains a systems of records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5 ,000.

Section 5.0 Sharing and Disclosure

- If it is unknown whether or not systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the systems/applications. As an example, if your system/application shares data with another system/application, ask yourself whether you have access to the data in the interfaced system/application. If so, then your answer is yes and an explanation is needed.
- Also consider "other" users who may not be obvious as those listed, such as GAO or the Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act system of records notice under the "Routine Use" section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.
- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

Section 6.0 Access and Security

- Access to data by a user (i.e. employee or contractor personnel) within FHF A is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a

need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.

- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.
- The system owner is responsible for ensuring that access to infom1ation and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system and/or application. However, restrict access when users do not need to have access to all the data.
- When a contract provides for the operation of a system on behalf of FHF A, the Privacy Act requirements must be applied to such a system. Contact the Contracting Officer or Contracting Officer's Technical Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The IT Security Certificate and Accreditation (C&A) process requires a system security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of systems to ensure that only authorized users can access the system for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the system can in fact monitor use of the system. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability to access a system is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring..
- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of system activity and user activity including invalid logon attempts, access to data and monitoring .The C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.
- According to OMB Circulars A-123 and A-130, every system/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data. For instance, in computerized systems the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the system and is transparent to the user. Describe these processes in response to this question.
- All employees, including contractors, have requirements for protecting information in Privacy Act systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

PIA FORM

Overview

This section provides an overview of the system and addresses the following:

- The system name and the division/office that owns the system;
- The purpose of the program, system, or technology and how it relates to the agency's mission; and
- A general description of the information in the system.

Date submitted for review:

Name of System:

System Owner(s) (including Division/Office):

Name	E-mail	Phone#
Joel Sackett (Office of Human Resources Mgmt)	Joel.Sackett@fhfa.gov	202-408-2858

System Overview: Briefly describe the purpose of the program, system, or technology, and the information in the system, and how it relates to the agency's mission.

The Plateau Talent Management System (TMS) supports agency efforts in relation to Office of Personnel Management (OPM) Guide to Human Resources Reporting (Enterprise Human Resources Reporting Integration – EHRI) and the e-Government Human Resources Line of Business – Human Resource Development (HR LoB/HRD). The TMS is based on a Commercial Off-The-Shelf (COTS) software application that manages web-based and classroom-based learning activities. The major functions of the system include providing access to commercial and agency-specific web-based courseware, managing an on-line catalog of course offerings; automating training registration and approval processes; on-line individual development planning; on-line testing and surveys; tracking of training resources; management of and reporting on training data; and tracking of training certifications. It supports the FHF A mission by assisting employees with professional and personal development.

The TMS was purchased through an Interagency Agreement with the National Technical Information Service (an OPM approved HR LoB/HRD Customer Service Providers (CSPs). The TMS is hosted externally at Plateau's hosting facility which has also been approved by OPM. OPM issues and maintains the Certification and Accreditation (C&A) for this TMS and the FHFA CIO signed the Authority to Operate (ATO) on 4/8/2011.

along with the system owner and CISO,

Learner data (FHFA employees and contractors) is maintained within the TMS. Appendix A contains a table of the data elements for each of these populations.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the system?	The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc. maintained due to OPM reporting requirements. The SSN and the RNO data are maintained in a privacy table not accessible to anyone through the application interface. Information on FHF A contractors is much more limited as we do not need the same level of detail for reporting purposes. (See Appendix A)
1.2	What are the sources of the information in the system?	For federal employees, the data in the system will come from the National Finance Center (NFC) and FHFA's Active Directory (AD). For contractors, the data will come from FHFA's Active Directory (AD).
1.3	Why is the information being collected, used, disseminated, or maintained?	The TMS is used to collect information on the training and development conducted or sponsored by FHF A for its employees and contractors.
1.4	How is the information collected?	As in 1.2 above, the data will be downloaded from NFC and AD and transferred via Secure File Transfer Protocol (SFTP) to Plateau's hosting/data center for upload into FHFA's TMS.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	The privacy risks are that the data might be compromised through unauthorized access to the TMS. The first mitigation factor is that the majority of the collected information that is maintained in the TMS is either available internally to other FHFA employees (through the AD/Outlook) or would be disclosed to the public pursuant to a FOIA request. The more sensitive data (SSN and RNO) is not available through the TMS, only via the secure encrypted privacy tables that exist within the database.

Section 2.0 Uses of the Information

The following questions delineate the uses of information and the accuracy of the data being used.

#	Question	Response
2.1	Describe the uses of information.	The application captures the information necessary to uniquely identify each user and the training they are required to take, have requested, and/or have completed. OPM policy also requires the collection and reporting of training data for all Federal employees. In addition, maintaining detailed information about the training offered by FHF A and or attended by FHFA employees 1s necessary to respond to training information requests, reporting requirements, and to measure human resource development program effectiveness.
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	The FHFA TMS architecture has implemented a domain structure and domain restrictions that limit TMS administrators' ability see learner data based on an established functional need. The TMS also automatically limits supervisor' view and reporting privileges to only those learners that fall beneath them in the chain of command. As a web-based application, all interaction and exchange of data is done through a secure site using 128-bit encryption.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is information retained	Information will be retained in the database until required to be deleted by the dates specified in 3.2 below.
3.2	Has a retention schedule been approved by the Agency's Records Management Officer and NARA? If yes, provide the corresponding GRS or Agency specific Records Schedule number.	NARA Records Schedule 1 (Section 29) describes records retention for agency sponsored training and employee training information. For agency sponsored training, destroy when 5 years old or 5 years after completion of a specific training program. For employee training, destroy when 5 years old or when superseded or obsolete, whichever is sooner (NC 1-64-77-10 item 30c)

#	Question	Response
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The only risk identified is that data will remain in the system after employees have separated the agency or retired from the federal government. This will be mitigated by inactivating the employee records so that it is not easily searchable through the application. This data will remain in the database in accordance with the records schedule in 3.2 above.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number	OPM has published a government-wide SORN that covers training records about federal employees (including contractor and volunteers) at 71 F.R. 35342 (June 19, 2006) (OPM/GOVT-1, General Personnel Records).
4.2	Was notice provided to the individual prior to collection of information?	The information was collected at the time the employee was hired by FHFA.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	The information is automatically collected from the National Finance Center and Active Directory databases. Individuals do not have an opportunity to decline to provide information.
4.4	What are the procedures that allow individuals to gain access to their information?	Much of the information (except data in the privacy tables) is viewable by the employee within their user records/talent profile by logging into the TMS.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Employees may request a review of information in the system by sending a request to the Q5 Help Desk at Q5Support@fhfa.gov or via phone to 202-408-2860. A TMS Administrator will research the data with the appropriate personnel or IT related systems and make any necessary modifications/corrections.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	Training data and statistics from the TMS are shared with various offices within FHF A due to mandatory training requirements such as Ethics, No Fear Act, Information Security Awareness, and Privacy Act.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	Enterprise Human Resources Integration (EHRI) training data is reported for Federal employees on a monthly basis in accordance with the OPM Guide to Human Resources Reporting. This information is transmitted through a SFTP system in an encrypted format.
5.3	Is the sharing of PII outside the agency compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? If so, describe. If not, describe under what legal authority the program or system is allowed to share PII outside of the agency.	Training data shared outside of FHFA is required by regulation. A list of the data elements required to be reporting to OPM is contained within Appendix B.
5.4	Given the external sharing explain the privacy risks identified and describe how they were/are mitigated.	Sharing with OPM creates the risk of unauthorized access for the information which includes Social Security Number. This risk is mitigated by the use of SFTP and data encryption. The OPM EHRI Program Management Office is responsible for ensuring an adequate level of protection and security is afforded to EHRI systems.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the system? Are these procedures documented in writing? If so, attach a copy to this PIA.	The system has two sites, a user site and an administrator site. All employees and contractors will access the user site, while only a select number of FHFA employees will have access to the Administrator Site. The Plateau PIA. TMS Solutions Design Document outlines the roles and functional responsibilities of users and administrators. (See attached TMS SDD).

#	Question	Response
6.2	Will contractors have access to the system? If yes, how will contractors gain access to the system? How will the agency control their access and use of information? Are there procedures documented in writing? If so, attach a copy to this PIA.	Since the system is being hosted by Plateau, their technical resources that manage the use of hardware/software at the hosting/data center could access our data. They receive the secure encrypted data file and load the information into the privacy tables, and then pull the data back out for the monthly reporting to OPM. The standard connector process is described within the Plateau Standard EHRI User Connector Requirements Workbook (see supporting documentation attached to this PIA).
6.3	Describe the training that is provided to users either generally or specifically relevant to the program or system?	All TMS users will be provided with a Quick Reference Guide, Frequently Asked Questions, function specific Job Aids and a robust Help System available within the TMS. Additionally, demonstrations for FHFA employees will be offered during the week the system is launched. Administrators will also receive a number of Job Aids and more formal training on their responsibilities within the system.
6.4	What technical safeguards are in place to protect the data?	Data is secured in accordance with FISMA requirements. Additionally, technical safeguards to prevent misuse of data maintained in the TMS include workflow and domain restrictions associated with every TMS administrator account. At Plateau's hosting facility, physical access 1s limited to key system hardware and system activity is monitored.
6.5	What auditing measures are in place to protect the data?	The Plateau TMS date stamps transactions such as reports that are run and user/admin logins. The database will show access and modifications to data.
6.6	Has a C&A been completed for the system or systems supporting the program? If so, provide the date the last C&A was completed.	Yes, a C&A has been completed by the Office of Personnel and is valid until re-certification is required in August 2012. The most recent OPM C&A was reviewed by FHF A IT Security Staff and Contractors and an Authority to Operate was signed by the FHFA CIO on 4/8/2011.

Signatures

Joel Sackett		6/8/2011
System Owner (Printed Name)	System Owner (Signature)	Date
N/A		
System Developer (Printed Name)	System Developer (Signature)	Date
Ralph Mosios	Ralph Mosios	6/9/2011

Chief Information Security Officer (Printed Name)	Chief Information Security Officer (Signature)	Date
R. Kevin Winkler		6/17/11
Chief Information Officer (Printed Name)	Chief Information Officer (Signature)	Date
David A. Lee		6/30/2011
Chief Privacy Officer (Printed Name)	Chief Privacy Officer (Signature)	Date