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 10 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 FHFA 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)(1).
- 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 (12 CFR Part 1204) 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 FHFA 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 information 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 FHFA, 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: June 3, 2011

Name of System: Plateau Talent Management 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 FHFA 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.

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.

along with the system owner and CISO

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?	For federal employees, this data includes names, work address and other information publically available on federal employees, as well as gender and Race and National Origin (RNO) pursuant to EEOC Management Directive 715. Additionally, the employees Social Security Number (SSN) is 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 FHFA 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 FHFA 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 use 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 FHFA and or attended by FHFA employees is 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 supervisors' 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 (NC1-64-77-10 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 FHFA 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 TMS Solutions Design Document outlines the roles and functional responsibilities of users and administrators. (See attached TMS SDD)
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 hardware/software at the hosting/data center could access our data. They receive the secure encrypted data file and load the information into

#	Question	Response
		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 is 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 FHFA IT Security Staff and Contractors and an Authority to Operate was signed by the FHFA CIO on 4/8/2011.

Signatures

Joel Sackett	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

Plateau Talent Management System Data Elements

Privacy Impact Assessment - Appendix A

Plateau Field	Description	FHFA Employee	FHFA Contractor	Administrator
User ID	The user's FHFA network ID from Active Directory (generally = last name + first initial)	X	X	X
First Name	The user's first name	X	X	X
Last Name	The user's last name	X	X	X
Middle Initial	The user's middle initial	X	X	X
Gender	The user's gender (male/female)	X		
Job Position	The user's position identifier (master record number) from NFC	X		
Job Title	The user's job descriptive job title.	X	X	
Role	Code identifying self-service access rights provided to the user (e.g. employee, contractor)	X	X	
Job Location	Code representing the city, state, and zip of the user's work location	X	X	
Domain	Code identifying domain assignment for user which determines visibility to record by TMS administrators	X	X	X
Organization	The user's organization code (based on the office they are assigned)	X	X	
Employee Type	Code indicating if user is permanent or temporary	X		
Employee Status	Code indicating if user is full-time or part-time	X		

Office Address	The user's work address including city, state, zip, country, and region	X	X	
E-mail Address	The user's email address used to send notifications to the user	X	X	X
Hired Date	Entry on Duty, the start date of the user	X		
Terminated Date	The last day of employment at the organization for the user. Date in this field makes user record inactive.	X	X	
Supervisor	First level supervisor's user ID	X	X	
Account Code	The Cost Center code for the user's assigned office	X		
Office Phone	The user's work phone number	X	X	
Social Security Number	The user's SSN (pulled from NFC). The value is not visible in the TMS but is maintained in an encrypted privacy table and will be used for OPM reporting purposes only.	X		
Date of Birth	The user's DOB (pulled from NFC). The value is not visible in the TMS but is maintained in an encrypted privacy table and will be used for OPM reporting purposes only.	X		
Salary	The user's salary	X		
Race and National Origin	The user's RNO Code (pulled from NFC). The value is not visible in the TMS but is maintained in an encrypted privacy table and will be used for OPM reporting purposes only.	X		
Supervisory Status	Code showing if the user is in a supervisory position	X		
Pay Plan	The user's pay plan	X		

Occupational Series	The user's series	X		
Grade	The user's current grade	X		
Education Level	The highest level of education attained by the user.	X		
Second Level Supervisor	Second level supervisor's user ID	X		
Retirement SCD	The user's retirement service computation date (pulled from NFC)	X		
Date Entered Current Grade	The user's most recent promotion date	X		
Tenure	The user's tenure in the federal government (e.g., career, career-conditional)	X		
Position Occupied	Code for the user's position (e.g., competitive, excepted)	X		

Office of Personnel Management (OPM) EHRI Data Fields

Privacy Impact Assessment - Appendix B

Chapter 4 of the OPM Guide to Human Resources Reporting contains specific information on the preparation and submission of training data files. Chapter 4 can be accessed at http://www.opm.gov/feddata/ghrr/ghrr07_ch4.pdf. Following are the 27 data fields required by EHRI.

	Data Concept	Name	Definition
1	Data Record	Record Action	Indicates action to take with this data record.
2	Employee ID	Social Security Number	Person's social security number.
3	Employee ID	Birth Date	Date on which the person is born.
4	Employee ID	EHRI Employee ID	The unique number that EHRI will assign to an employee to identify employee records within the EHRI.
5	Employee ID	Agency Subelement Code	Agency and, where applicable, the administrative sub-division (i.e., subelement) in which a person is employed.
6	Completed Training Unit	Training Title	Official title or name of the course or program completed by the employee.
7	Completed Training Unit	Training Type Code	Code for the type of training which has been completed by the employee.
8	Completed Training Unit	Training Sub Type Code	Code for the type of training which has been completed by the employee.
9	Completed Training Unit	Training Start Date	Start date of the training completed by the employee.
10	Completed Training Unit	Training End Date	End date for the training completed by the

			employee.
11	Completed Training Unit	Continued Service Agreement Expiration Date	The date to which an employee is obligated to remain in service as a stipulation for taking the training course.
12	Completed Training Unit	Continued Service Agreement Required Indicator	Indication that an employee is obligated to remain in service as a stipulation for taking the training course.
13	Completed Training Unit	Training Accreditation Indicator	Indicates if the training course offers accreditation.
14	Completed Training Unit	Training Credit	Amount of academic credit hours or continued education units earned by the employee for the completed training.
15	Completed Training Unit	Training Credit Designation Type Code	Code for the type of academic credit hours or continued education units earned by the employee for the completed training course.
16	Completed Training Unit	Training Credit Type Code	Code representing the type of credit hours the employee received for the completed training.
17	Completed Training Unit	Training Duty Hours	Number of employee duty hours the employee used to complete the training unit.
18	Completed Training Unit	Training Non Duty Hours	Number of employee non-duty hours for the completed training course.
19	Completed Training Unit	Training Delivery Type Code	Code for the type of training delivery for the training course completed by the employee.
20	Completed Training Unit	Training Purpose Type Code	Code representing the purpose of the training completed by the employee.
21	Completed Training Unit	Training Source Type Code	Source of the training which has been completed by the employee.
22	Training Material Costs	Training Materials Cost	Cost to the Government for the training

			materials used during the training unit completed by the employee.
23	Training Per Diem Cost	Training Per Diem Cost	Cost of the per diem (meal, lodging, misc. expenses) for training completed by the employee that was paid for by the Federal Government.
24	Training Travel Cost	Training Travel Cost	Cost for the travel, excluding per diem, for training completed by the employee that was paid for by the Federal Government.
25	Training Tuition and Fees Cost	Training Tuition and Fees Cost	The cost of the training tuition and fee for training completed by the employee that was paid for by the Federal Government.
26	Training Nongovernment Contribution Cost	Training Nongovernment Contribution Cost	Cost contributed by the employee or other non-government organizations for the training completed by the employee.
27	Training Travel Indicator	Training Travel Indicator	Indicates if the employee traveled to attend the training course.

1.1 Role Management

1.1.1 Workflows

Admin roles consist of workflows – the combinations of functions (actions) and entities that grant system rights. There are over 800 possible workflows that could be assigned to an Admin role, many of which are individually available for domain restriction if required. Determining which workflows Admin roles should have is a challenging process and considerable time and resources should be invested in building and testing the Admin roles to perform the needed functions while keeping security and record access in place.

Admin Role

Function	Entity	Domain Restriction
Search	Item	A,C-2
View	User	
Add	Curriculum	B,C,D
Edit	Scheduled Offering	C-1,C-2,C-3,C-4
Delete	Catalog	

Each workflow may be restricted by domain, but only by one domain restriction record. This why domain restrictions contain more than one domain, and can contain any combination of domains. In the above example, Admin roles with the 'edit Scheduled Offering' workflow can edit offerings in the C-1, C-2, C-3 and C-4 domains (because those domains are referenced in that domain restriction record). The Admin role's 'view User' workflow is unrestricted. This Admin role may view all Users in the system.

1.1.2 Admin Roles

Admin roles consist of selected workflows with (or without) applied domain restrictions. Remember, domain restrictions are not applied to the Admin role – they are applied to each individual workflow within the role. Administrator roles are assigned to administrator accounts which in turn allow individual administrators access to Plateau. Admin accounts may have multiple Admin roles, as workflows do not interfere with each other. The Admin always has the combination of access provided by all assigned roles.

Listed below are the Admin Roles to be created by FHFA along with notes from workshop discussions.

System Admin > Security > Role Management

Role ID (30 Char)	Description (100 Char)
SYSADMIN	*The default role with full access.*
REPORT	*Report Only Administrator will have access to reports only.*
VIEW	*View and search access to the Plateau LMS.*
TA	*Training Administrator who manages users' SF-182s and run reports on user activities.*

Notes
Create and test the generic roles. Make a copy of the roles and create a separate role for each domain

Notes
set - Identify roles per domain restriction or office. For example: Training Administrator for OIG = TAOIG Training Administrator for DO = TADO Training Administrator for OIA = TAOIA Organization Owners (users) will have the ability to drill down on item completions, goal completions, curricula status. These persons will be set up, from their user records, to view these elements.

1.1.3 User Roles

User Roles, like Admin Roles, are used to grant access in the Plateau application. However, User Role workflows are primarily access to menus and Easy Links – not to records. There are no Domain Restrictions to apply. Typically, there is only one User Role (Default User) applied to all Users in an implementation. Sometimes there are needs recognized to grant different levels of menu access to different groups of Users. In which case, additional User Roles may be created and assigned automatically via Assignment Profiles to all the Users who match certain attributes. User Roles may also be assigned manually to individual Users.

Note: It is not necessary to create separate User Roles for Supervisors as they are subject to the User Role assigned to them and also the User Assumption Restriction Rules specified in the configuration xml file.

System Admin > Security > Role Management

Menu	FHFAUSER	Contractor
Admin		
Admin Home	X	
Reports		
Search Reports	X	
Career		
Access Competency Assessment History	X	
Access Career Planner [1]		
Access Competency Assessment Processes [3]	X	
Access Competency Assignments	X	
Access My Plan [1 or 2]	X	
Access Performance Reviews [2]		
Initiate Multi-Rater Assessments [3]	X	
Catalog		
Access Advanced Catalog Search	X	X
Access Browse Catalog	X	X
Access Calendar of Offerings	X	X
Access Simple Catalog Search	X	X
Learning		
Access Current Enrollment	X	X
Access Qualification Status	X	X
Access External Learning Requests [7]	X	
Access Learning Calendar	X	X
Access Learning History	X	X
Access Learning Plan	X	X
Access Plateau Offline Learning [8]		
Access Questionnaire Surveys	X	X

Menu	FHFAUSER	Contractor
Access Record Learning Events		
My Employees		
Cancel Subordinate Performance Review [2]		
Manage Alternate Supervisors	X	
Access My Plans [1 or 2]	X	
Access Employee Matrix	X	
Access Learning Plans	X	
Access Registrations	X	
Access Subordinate Competency Assessment Processes [3]	X	
Access Subordinate Deadline Dashboard	X	
Access Subordinate Goal Status Dashboard [1 or 2]	X	
Access Subordinate Performance Review Status Dashboard [2]		
Access Subordinate Performance Reviews [2]		
Access Subordinates	X	
Organization [4 or 5]		
Access Dashboard		
Access Initiatives [4]		
Access Succession Planner [5]		
Access Talent Pool		
Performance Management		
Access Advanced Career Planner [1]		
Access Development Planning [1]	X	
Access Goals Alignment [4]		
Access Performance Planning [2]		
View Review History [2]		
Access Plateau Offline Multi Rater/360 [6]		
Personal		
Access Approvals	X	
Access Easy Link 1	X	
Access Easy Link 10	X	
Access Easy Link 2	X	
Access Easy Link 3	X	
Access Easy Link 4	X	
Access Easy Link 5	X	
Access Easy Link 6	X	
Access Easy Link 7	X	
Access Easy Link 8	X	
Access Easy Link 9	X	
Access Home	X	X
Access Communities		
Access News	X	X
Access Order Status		
Access Order Tickets		
Access Talent Gateway [10]		
Access Profile	X	
Access User Settings	X	
Access Shopping Cart		
Access Skills		
Reports		

Menu	FHFAUSER	Contractor
Access Reports	X	

Note: License Dependencies (Selected workflows are not available without associated product licenses):

[1] Career and Development License Required

[2] Performance Goals and Appraisals License Required

[3] 360° Multi-Rater Assessments License Required

[4] Goal Alignment License Required

[5] Succession Planner License Required

[6] 360° Multi-Rater Assessments and Plateau Offline Player Licenses Required

[7] External Learning Requests (SF_182)

[8] Plateau Offline Player

[9] Compensation

[10] Talent Gateway

1.1.4 Delegate User Role

The delegate user role is assigned to a user who has been selected by a supervisor. The delegate will have most of the rights of the supervisor. The global setting for the delegate can be controlled from the User Proxy Role.

Menu	Delegate User
Career	
Access Competency Assessment History	x
Access Career Planner [1]	x
Access Competency Assessment Processes [3]	x
Access Competency Assignments	x
Access My Plan [1] or [2]	x
Access Performance Reviews [2]	x
Initiate Multi-Rater Assessments [3]	x
Catalog	
Access Advanced Catalog Search	x

Menu	Delegate User
Access Browse Catalog	x
Access Calendar of Offerings	x
Access Simple Catalog Search	x
Learning	
Access Current Enrollment	x
Access Qualification Status	x
Access External Learning Requests [7]	x
Access Learning Calendar	x
Access Learning History	x
Access Learning Plan	x
Access Questionnaire Surveys	x
Access Record Learning Events	x
My Employees	
Cancel Subordinate Performance Review [2]	x
Access My Plans [1 or 2]	x
Access Employee Matrix	x
Access Learning Plans	x
Access Registrations	x
Access Subordinate Competency Assessment Processes [3]	x
Access Subordinate Deadline Dashboard	x
Access Subordinate Goal Status Dashboard [1 or 2]	x
Access Subordinate Performance Review Status Dashboard [2]	x
Access Subordinate Performance Reviews ****	x
Access Subordinates [2]	x
Performance Management ****	x
Access Advanced Career Planner [1]	x

Menu	Delegate User
Access Development Planning [1]	x
Access Goals Alignment [4]	x
Access Performance Planning [2]	x
View Review History [2]	x
Personal	
Access Approvals	x
Access Easy Link 1	x
Access Easy Link 10	x
Access Easy Link 2	x
Access Easy Link 3	x
Access Easy Link 4	x
Access Easy Link 5	x
Access Easy Link 6	x
Access Easy Link 7	x
Access Easy Link 8	x
Access Easy Link 9	x
Access Home	x
Access Profile	x
Access User Settings	x
Access Skills	x
Reports	
Access Reports	x

Excerpt from FHFA Plateau EHRI User Connector Requirements Workbook

Interface General Design

1.2 Introduction

The business rules incorporated into the standard connectors are formulated by Plateau based on the needs of the typical Plateau customer. This pre-developed code is packaged to be deployed on a customer site without any customizations. The standard connectors call for the Customer source data to be formatted in the pre-defined standard connector format.

The purpose of this document is to describe the functions of the standard connector. It describes the process for customers to produce data in an acceptable format so it can be transferred and stored in Plateau's database. The following should be noted by all parties involved in the standard connector implementation.

- This document defines the requirements for the connector. If you have unique business requirements/rules beyond what is specified, please bring this to your Project Manager's attention as a custom connector may need to be implemented. If a custom connector is needed a Change Order will be developed to include development, testing and deployment support hours. Note that it is not recommended by Plateau to go with a custom solution due to the increase in timeline, cost and risk.
- There are several decisions the customer must make within this document that will ensure that the connector is set up and runs properly, however these decisions will not result in any modifications to the code. These questions are highlighted in a red font.
- The required fields included within the standard connector are not negotiable. Fields that cannot be null must have a value passed from a legacy system into the source data file. These fields are noted in the data mapping table. Additional fields may be added within the specified allowable number of custom columns.

The standard connector can be used for a one time data conversion or for an on-going connector interface.

1.3 Standard Connector Process

A high level summary of the seven data conversion steps are listed below. There are three main participants in this process which include the Customer Business Owner, Customer Source File Owner, and Hosting Department (either Plateau if Customer is hosted or the Customer Hosting Department). Sections of this document are focused on these participants.

Step	Action	Owner
1	Complete configuration of custom fields.	Customer Business Owner
2	Take snapshot of schema to include reference field configuration in Step 1.	Hosting Department
3	Provide data file to Plateau Project Manager. If you are a Plateau hosted customer there are two recommended approaches for the customer to send a data conversion source file to Plateau. If the file is small enough, it can be e-mailed to the Plateau Project Manager. If it is larger it should be made available via the CSO FTP site.	Customer Source File Owner
4	Data Validation script run against input file. If data file elements are invalid, return to customer with recommendations. Validate subsequent input files.	Plateau Tech Lead
5	Install connectors	Hosting Department
6	Run connector	Hosting Department
7	View the log reports and records via the user interface to verify the conversion. *Note: If there are data anomalies not found in Step 4, the reports will include errors to suggest modifications to make to the data file or reference fields in the TMS prior to rerunning the scripts.*	Plateau Consultant, Customer Business Owner, and Customer Source File Owner

Federal Housing Finance Agency
1700 G Street, N.W., Washington, D.C. 20552-0003
Telephone: (202) 414-3800
Facsimile: (202) 414-3823
www.fhfa.gov

April 8, 2011

MEMORANDUM FOR: Kevin Winkler, Authorizing Official
Chief Information Officer, FHFA

FROM: Ralph Mosios, Certifying Official
Chief Information Security Officer, FHFA

SUBJECT: **Security Certification for Plateau Learning Management System (Plateau LMS)**

The FHFA IT Security Team was tasked with reviewing the Office of Personnel Management (OPM) Plateau LMS application certification & accreditation (C&A) package. My team determined that the C&A package was conducted in accordance with OMB Circular A-130 and NIST Special Publications 800-37 and 800-53.

The FHFA IT Security Team assessed the OPM C&A package to determine the extent to which management, operational, and technical security controls are sufficiently documented and are producing the desired outcome with respect to meeting security requirements. Since OPM conducted a full C&A, my team reviewed the existing C&A documentation to ensure consistency with FHFA's C&A program. The attached certification package contains:

- Risk Assessment Report
- Plan of Actions and Milestones (POA&M) Report

The Plateau LMS C&A package contained a risk assessment of the system's management, operational, and technical security controls and should be used as a basis for the accreditation decision. Therefore, I recommend that the Plateau LMS application be accredited until August 30, 2012 in its current state, at which time OPM will have completed their re-certification using NIST 800-53 Revision 3. Major changes to the system's configuration, security breaches or serious security violations may require a recertification before the end of the authorization period.

Ralph Mosios
Ralph Mosios
Certifying Official

4/8/2011
Date

Federal Housing Finance Agency
1700 G Street, N.W., Washington, D.C. 20552-0003
Telephone: (202) 414-3800
Facsimile: (202) 414-3823
www.fhfa.gov

April 8, 2011

MEMORANDUM FOR: Joel Sackett, System Owner
Senior Employee Development Specialist, FHFA
System Owner, USA Staffing

FROM: Kevin Winkler, Authorizing Official
Chief Information Officer, FHFA

SUBJECT: **Security Accreditation Decision for Plateau Learning Management System (Plateau LMS)**

After reviewing the results of the Plateau LMS Risk Assessment Report and the supporting evidence provided in the Office of Personnel Management (OPM) approved certification and accreditation (C&A) package, I have determined that the risk to agency operations, agency assets, or individuals is acceptable. Accordingly, I am issuing a full authorization to operate in the existing operating environment. This security authorization requires remediation of high risk findings in the system's POA&M within thirty (30) days of this accreditation.

Since OPM is not due to re-assess the Plateau LMS C&A package to be consistent with the latest National Institute of Technology and Standards (NIST) guidance, NIST-800-53 Revision 3, until August 2012, this authorization will remain in effect until August 30, 2012, or until significant change is made to the security controls or configuration warranting another review.

As Authorizing Official for the Plateau LMS, I authorize this system to operate.

Joel Sackett, OHRM
System Owner — Date: 4/8/11

Ralph Mosios, OTIM, CISO
Certifying Official — Date: 4/8/11

Kevin Winkler, OTIM, CIO
Authorizing Official — Date: 4/8/11