Privacy Impact Assessment Template

OFFICE OF INSPECTOR GENERAL
TEAMMATE

This template is used when the Chief Privacy Officer determines that an IT 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
400 7th Street SW
Washington, DC 20024
(202) 649-3803
Privacy@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form ("IIF"; also referred to Personally Identifiable Information (PII)) 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 System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/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.

FOR A PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- **Overview**
- **Section 1**
- **Section 2**
- **Section 6**

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:
  - 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 a private organization).
- If the System collects information from 10 or more members of the public, ensure that FHFA has received prior approval from OMB 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 FHFA's or the Office's/Division's/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 for 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, these 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 unique 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 Chief Privacy Officer.
- If a name or other unique 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 System 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 you do not know 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 the General Counsel Accountability Office or the FHFA Office of Inspector General. "Other" may also include database

administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN 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 Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The 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: September 13, 2012

System Name:			
System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Russell Rau	russell.rau@fhfaoig.gov	Office of Inspector General – Office of Audit	202-730-0390

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.

TeamMate is a commercial off-the-shelf suite of auditing software products combining both desktop and web-based technologies. The combined suite allows auditors to identify, schedule, document, report, and track time and expenses on audits using a modular approach. Each module can be installed and used independently with individual databases. However, when the modules are used together with the same database, the applications can interact and automate the entire audit workflow.

Information from TeamMate is used for documenting audit workpapers and to document various policies and procedures of the Office of Inspector General, Federal Housing Finance Agency (FHFA-OIG). Uses of the information would include support for audit and review reports; quality control review by third parties; and audits by GAO.

The following is a list of the applications that comprise the TeamMate suite:

- **TeamMate Electronic Work Papers (EWP)** – Desktop application used to manage workpapers in the auditing process;
- **TeamStore** – Desktop application used in conjunction with EWP to integrate imaging;
- **TeamRisk** – Desktop application allowing risk assessment on the audit universe to determine what to audit based on risk;
- **Team Risk Web** – Web application that allows business owners and distributed auditors to contribute to the risk assessment;

- **TeamSchedule** – Desktop application that allows schedulers to schedule projects and assign resources;
- **TeamSchedule Web** – Web application that allows users to view scheduled plans;
- **TeamMate Time and Expense Capture** – Web application that allows users to enter time and expenses related to a project;
- **TeamCentral** – Web application (data-mining) that allows teams and audit management to view reports on the status of projects and issues across audits; and
- **TeamAdmin** – Desktop application that allows TeamMate Administrators to perform various functions on the centralized database (included in a separate installation).

The TeamMate Suite is hosted on a secure, FHFA-OIG-dedicated physical server at the Washington, D.C. headquarters for the National Aeronautics and Space Administration's Office of Inspector General (NASA-OIG).

TeamMate typically does not include Personally Identifiable Information (PII), but the responses in this PIA apply to the unusual situations where PII is contained or may be contained in TeamMate.

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 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?	Any documentation that would support an audit or review could be collected and stored (maintained) on the TeamMate application database. TeamMate typically does not include PII, but if audit objectives were to require this, such potential PII could include but not be limited to social security numbers, addresses, telephone numbers, loan numbers and any other PII that could be collected by FHFA-OIG. Information from the system is only disseminated in audit or review reports or memos or similar types of communication. Information that could contain PII would reside in the TeamMate centralized database that would serve as support to audit reports and memos. TeamMate also contains FHFA-OIG policies, procedures, and reference documents.

#	Question	Response
1.2	What are the sources of the information in the System?	The sources of information include manually-inputted/typed data incorporated into TeamMate-provided forms by authorized FHFA-OIG users, and/or electronic workpaper files including scanned documentation, uploaded into TeamMate via the FHFA-OIG General Support System (GSS). The documentation could come from any person within FHFA, Fannie Mae, Freddie Mac, FHLBanks, Office of Finance, or other sources, including hotline complaints, GAO, and congressional requests.
1.3	Why is the information being collected, used, disseminated, or maintained?	The information serves as supporting documentation for audits and reviews.
1.4	How is the information collected?	As noted in section 1.2, information is input/imported manually into TeamMate. Except for the GSS, no interconnected systems feed data into TeamMate. Information is usually provided by auditees as electronic files that would be imported into the TeamMate application database, and then encrypted by the TeamMate application. Additionally, some hard copy documentation is provided by auditees to FHFA-OIG. These would typically be scanned into an electronic file (usually Adobe Acrobat format), and then added to the TeamMate database (that would then become encrypted by the TeamMate application).
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Potential risks associated with the data could be privacy, financial risk, and reputation risks. However, these risks are minimized for several reasons (as detailed in Section 2.2).

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.	Information from TeamMate is used for documenting audit workpapers and to document various FHFA-OIG policies and procedures. Uses of the information would include support for audit and review reports; quality control review by third parties; and audits by GAO.

#	Question	Response
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.	All data is stored in a centralized database that works with MS SQL Server. All applications that might use this data connect to the centralized database using TeamMate "connection" files (.tmc). These XML-based files contain all the required database location and connection information. The TeamMate Suite database, when using MS SQL Server for the suite of applications, is not encrypted, which allows organizations to integrate with their own systems or import/export data as needed. However, documents contained in the database are encrypted. The centralized database is only exposed to the application and a small set of Database Administrators, minimizing the security risk. The Service-based databases (MS SQL Server) are centralized within FHFA's data center, and access to these databases is restricted to the minimum number of people needed to administer the database. TeamMate utilizes the authentication and authorization models of these databases to control access to the database. TeamMate allows different forms of authentication. FHFA-OIG uses the Windows form of authentication. Using this Windows (integrated) authentication, the TeamMate application is maintained on FHFA-OIG-dedicated physical secure servers hosted at NASA-OIG headquarters in Washington, DC. The host server issues RSA two-factor authentication to all users to prevent unauthorized access to the hosted environment and data. Windows Authentication will authenticate a user based on the standard windows login. When the user accesses the Web Application, the logged-in Windows account information is passed to the application for validation against the TeamMate global database. This process is automatic and does not require a user to enter any information into a form on the web page. If the user's Windows account information (ex: Domain\loginname) matches a login name in the database for this application

#	Question	Response
		then the user is allowed to continue into the web application (site). To utilize the RSA token, the user must provide a log-on name, an 8-digit unique PIN, the RSA token value (which changes every 60 seconds), and a minimum 12 character password requiring special characters, capital letters, and numbers. In addition, users are identified with session-specific IP addresses, such that the same username cannot be used simultaneously from another location. In addition to authentication controls, each individual user has specific access rights once admitted to the system. Persons granted access to TeamMate data have appropriate clearances and have signed the appropriate confidentiality statements aimed at preventing the unauthorized release of information. Such persons are assigned certain access rights within TeamMate applications and projects. Access rights vary, ranging from Administrative rights, preparer privileges (write access), read access, and no access allowed at all. Usernames and Passwords controls restrict authorized users from accessing the TeamMate centralized database and projects to which they lack permission to access. At the end of an audit, the TeamMate Administrator removes access rights to the TeamMate system and/ or audit file to any auditors who no longer need access. Typically, this would occur when contract auditors have completed the audit, but could also occur when FHFA-OIG auditors leave the agency. Additionally, TeamMate resides on the agency's GSS and also has all the inherent security controls associated with this system, including strong password controls and physical security controls. Were a breach to occur, the FHFA-OIG Deputy Inspector General for Audits (DIGA) would follow all currently required FHFA-OIG procedures, taking all appropriate steps to assess the impact of the breach, to notify affected

#	Question	Response
		persons, and to prevent future breaches in accordance with FHFA-OIG policies on the protection of PII, breach response, and IT infrastructure.

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?	FHFA-OIG-specific records (including all audit, supporting workpapers, and policy-related documentation), as well as any agency-specific records held by FHFA-OIG, are retained in accordance with the FHFA Records Retention Schedule (May 30, 2011), which provides that Audit Records are destroyed or deleted 7 years after cutoff, *i.e.*, when the project, activity or transaction is completed or superseded.
3.2	Has a retention schedule been approved by FHFA's Records Management Officer and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	OIG follows the FHFA Records Retention Schedule, which is currently under review by NARA.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Since there are controls over access to the data (where documents are encrypted in the centralized database on the secure server at NASA) as well as read and/or write access levels controlled by the system administrator, the risks are low that length of time on the database would have any impact. Additionally, information is only retained as long as required under the FHFA Record Retention Schedule (see responses to 3.1 and 3.2).

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. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	Yes – FHFA-OIG-1, "FHFA-OIG Audit Files Database." Either this SORN will be updated or a new SORN will be issued to cover the new hosting arrangement.

#	Question	Response
4.2	Was notice provided to the individual prior to collection of information?	Notice is typically not provided in an audit or review, because, in the course of its work, FHFA-OIG seeks records in the possession of the agency or contractors, rather than those in possession of individuals in their capacity as such. For example, an FHFA employee would not be informed if his/her name was included in a Payroll Audit sample.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	No; see response to Question 4.2.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may request access to their information by filing a request pursuant to the Freedom of Information Act or the Privacy Act in the manner prescribed in applicable regulations and procedures. Such requests are processed in accordance with these authorities.
4.5	What are the procedures for correcting inaccurate or erroneous information?	In the case of disseminated records, individuals may make a request for correction to the FHFA-OIG Chief Counsel. In the unlikely event that material information in TeamMate constituted Privacy Act records, such material would be subject to the Act's amendment process, to the extent that the material was not exempt.

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?	Information included in or derived from TeamMate could be potentially shared with the FHFA-OIG Office of Investigations (to avoid duplicating and/or compromising investigations), the FHFA Director, FHFA executive management, an office director or directors, and/or FHFA auditees on a need to know basis. Information may also be shared pursuant to Privacy Act routine uses.

#	Question	Response
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.	Information could be potentially shared with law enforcement officials, such as in the event of an investigation, where investigators may need to review documentation related to an audit. Additionally, information will be shared with contractor auditors that perform work for FHFA-OIG. Controls on contract auditors are discussed in Section 6.2 below. Further, TeamMate provides support for audit and review reports; quality control reviews by third parties; and audits by GAO.
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? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	FHFA-OIG does not share PII apart from routine uses under the Privacy Act, and does not anticipate any further sharing. Sharing of non-Privacy Act records would be done in accordance with the Freedom of Information Act (and its exemptions for protecting personal privacy interests), and, in the course of litigation, the Federal Rules of Civil Procedure or equivalent.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Potential risks associated with the data could be privacy, financial risk, and reputation risks. Information is protected as discussed in section 6.2 below with regard to FHFA-OIG contract auditors. Other recipients are organizations similar to FHFA-OIG who maintain shared information in secured record systems, such as law enforcement organizations.

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? <u>If so, attach a copy to this PIA.</u>	See response to question 2.2 above. These procedures are documented in the OIG TeamMate User Guides.
6.2	Will non-FHFA personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will the agency control their access and use of information? Are there procedures documented in writing? <u>If so, attach a copy to this PIA.</u>	Contractors may access TeamMate if approved by the DIGA or his designee. All controls on authentication and access described in Section 2.2 will apply to contractor access. All contract auditors undergo OPM background checks, sign statements of independence, and have the same TeamMate and GSS credentialing process as FHFA-OIG users. There is no effective difference between a contract auditor accessing

#	Question	Response
		TeamMate and an FHFA-OIG auditor doing the same.
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	All employees complete annual Privacy Awareness training, and contractors are required to sign confidentiality statements.
6.4	What technical safeguards are in place to protect the data?	See response to question 2.2.
6.5	What auditing measures are in place to protect the data?	As soon as projects are completed, the projects are "finalized", *i.e.*, all data is write protected, which is performed by the TeamMate Application Administrator. In addition, any documents containing PII are protected by being designated as "Confidential" in TeamMate, so only those with the same role level or higher can access the file. This will be performed by the TeamMate File Project Owner, who will designate only the DIGA as having the same level (Administrator), which would preclude anyone but the DIGA, TeamMate File Project Owner, and TeamMate Application Administrator from accessing the file. As soon as contract employees complete their audits on TeamMate, they are removed from the GSS, which would also prevent them from accessing the TeamMate project files. Contractors will be required to utilize OIG-issued laptop computers, which do not permit the downloading of TeamMate files to CDs. The only way to retrieve data from the laptop is the requirement to use OIG-issued encrypted USB thumb drives. Users are notified of this practice in training on the OIG IT Rules of Behavior. Confidentiality Agreements are signed at contract inception with the contractors working with FHFA-OIG. These agreements require the return of unneeded Confidential Data to the DIGA or the Audit Director, or notification to either of them about the destruction of such data. "[U]nneeded" and "Confidential Information"

#	Question	Response
		are defined in the Confidentiality Agreements; the definition of Confidential Information is broad enough to include PII. Written OIG policy restricts users from emailing PII in the body of an email message –PII may only be sent in a separate encrypted attachment to email. Any hard copies of PII-type records would be stored in locked file cabinets in the FHFA-OIG area. At the conclusion of a contract audit, all original working papers become the property of OIG. The practice for this return is to obtain a .zip file of the contractor-performed work papers and import the file into the FHFA-OIG TeamMate Oversight file.
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. If not, and one is required, provided the expected completion date of the C&A.	Yes. A C&A for the secure hosting and storage facility at NASA was last completed on September 29, 2010. FHFA issued an Authorization to Operate for TeamMate on December 16, 2011.

Signatures

Russell Rau		9/14/12
System Owner (Printed Name)	System Owner (Signature)	Date
DAVID BONORCHIS		9/18/2012
Chief Information Security Officer (Printed Name)	Chief Information Security Officer (Signature)	Date
DAVID BONORCHIS		9/18/2012
Chief Information Officer (Printed Name)	Chief Information Officer (Signature)	Date
David A. Lee		9/18/2012
Chief Privacy Officer (Printed Name)	Chief Privacy Officer (Signature)	Date