Privacy Impact Assessment
for the

TeamMate

February 11, 2008

System Owner
Jay Jacobsen
FHFB OIG
202-408-2544, jacobsenj@fhfb.gov

Reviewing Official
David Lee
Chief Privacy Officer
Federal Housing Finance Board
Leed@fhfb.gov

Overview

This section fulfills the E-Government Act's requirement for an introduction for members of the public who will be reading the PIA (in theory, this PIA could be read by members of the public, although in practice this rarely happens—if ever). The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the system owner's responses in the PIA. Ultimately, the audience for the PIA will consist of members of the public who are unfamiliar with the technical details of the system. The overview should contain the following elements:

- The system name and the name of the Finance Board program(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the Finance Board's mission;
- A general description of the information in the system.

TeamMate is an electronic working paper commercial off the shelf (COTS) application used for audit purposes. Information from TeamMate is used for documenting audit workpapers and to document various 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.

TeamMate contains 6 different modules, of which only one (TeamMate EWP) is used for storing documentation from Auditees. TeamMate EWP resides on the FHFB network. All data stored on the application database is saved in network folders in encrypted files. Access to the various projects is controlled by the TeamMate Administrator, who controls the level of access for the users. In order to access project data, the system administrator must first set up a user on the system. The user has a password for accessing the project. Additionally, the system administrator provides certain access rights to that user: preparer/reviewer rights (write access and approval), preparer (write access only), and read access. The other five modules, which are not used for document storage include:

- TeamStores
- TeamRisk
- TeamSchedule
- TeamMate Time and Expense Capture
- TeamCentral

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, rule, or technology being developed. The questions address all information collected, with more emphasis provided for any collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

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. Information from the system is not typically disseminated from the system other than in audit or review reports or memos or similar types of communication. Information that could contain PII would reside on the system in TeamMate-encrypted files that would serve as support to audit reports and memos. TeamMate also contains OIG policies, procedures, and reference documents.

As we have noted in the Overview section, 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, depending on the audit objectives.

1.2 What are the sources of the information in the system?

The documentation could come from any person within the FHFB, FHLBanks, Office of Finance, or other sources, including hotline complaints, GAO and congressional requests, etc.

1.3 Why is the information being collected, used, disseminated, or maintained?

Information would serve as supporting documentation to only audits and reviews.

1.4 How is the information collected?

Information is usually provided by Auditees as electronic files that would be added to the TeamMate application database in encrypted format. Additionally, some hard copy documentation is provided by Auditees to OIG. These would typically be scanned into an electronic file (usually Adobe format), and then added to the TeamMate database in encrypted files.

1.5 Privacy Impact Analysis: 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. First, TeamMate is designed to encrypt all electronic files that are stored on the database. Also, TeamMate has password controls to prevent individuals from accessing TeamMate projects that they do not have authorization to see. Also, even if auditors get access to certain TeamMate projects, access rights are assigned to each user. Access rights vary from Administrative rights, preparer privileges (write access), to read access, to no access allowed at all. Additionally, TeamMate resides on the agency's General Support System and also has all the inherent security controls associated with this system, including strong password controls, etc. Persons who have access to the data have appropriate clearances and have signed the appropriate confidentiality statements aimed at preventing the unauthorized release of information. If a breach occurs, the IG will follow all procedures at the time, and will take appropriate steps to assess the impact of the breach, take steps necessary to notify affected persons, and to prevent future breaches.

Section 2.0 Uses of the Information

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

2.1 Describe the uses of information.

Information from TeamMate is used for documenting audit workpapers and to document various 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.

2.2 Privacy Impact Analysis: Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.

See response to 1.5 above.

Section 3.0 Retention

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

3.1 How long is information retained?

Information is retained in accordance with OIG's approved retention schedule on file in the Office of Management. Additionally, a revised OIG retention schedule has been approved by OM, but currently under review by NARA. The revised OIG retention schedule would provide for audit case files disposition authority "Transfer to National Archives after 5 years. Destroy 9 years after cut off." Please refer to the current OIG record retention schedule for the retention period for all audit and policy related documentation.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. There is currently an OIG records retention schedule on the agency website that has been approved by the agency records officer and NARA. Additionally, as discussed in 3.1, the OIG has provided a revised records retention schedule that has been approved by the agency records officer, but is still being reviewed by NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Since there are access controls over access to the data (which is encrypted on the network) and 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 FHFB Record Retention Schedule (see responses to 3.1 and 3.2).

Section 4.0 Internal Sharing and Disclosure

The following questions define the scope of sharing within the Finance Board.

4.1 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 an office director, Board Member, chairman, or Auditees of the agency on a need to know basis.

Section 5.0 External Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing external to the Finance Board which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

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 is shared with contractor auditors that perform work for the OIG and TeamMate provides support for audit and review reports; quality control reviews by third parties; and audits by GAO.

5.2 Is the sharing of PII outside the Finance Board compatible with the original information collection? If so, is it covered by an appropriate routine use in a System of Record Notice? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of the Finance Board.

Currently, OIG does not share, outside of the Finance Board, any PII that might reside on TeamMate and does not anticipate any such sharing at this time. Should PII from TeamMate be shared outside of the Finance Board, and assuming the PII originated from material that constitute Privacy Act records as defined in that Act, then the sharing would consistent with routine uses set forth in the Privacy Act system of records notice FHFB-6 (SORN FHFB-6), Office of the Inspector General Audit and Investigative Files. Sharing of non-Privacy Act records would be done in accordance with the Inspector General Act, 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.

5.3 <u>Privacy Impact Analysis</u>: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Potential risks associated with the data could be privacy, financial risk, and reputation risks. Information is protected as discussed in section 1.5 above with regard to OIG contract auditors. Other recipients are organizations similar to OIG who maintain shared information in secured record systems.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 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, 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, a Finance Board employee would not be informed if his/her name was included in a Payroll Audit sample.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

No; see response to Question 6.1. Moreover, the Inspector General Act of 1978 gives OIG the right of access to all agency records, so there is no statutory right for agency officials to decline to provide such records to OIG in the course of its work.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may gain access to their information by filing a request pursuant to the Freedom of Information Act or the Privacy Act in the manner prescribed in the applicable Finance Board regulations and procedures.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals should contact the Finance Board's Privacy Act Official to gain access to their personal information.

In the case of disseminated records to which section 515 of the Treasury and General Government Appropriations Act, 2001 applies, individuals may make a request for correction pursuant to that statute and the Finance Board's section 515 regulations and procedures.

In the unlikely event that material information in TeamMate constituted Privacy Act records (as defined in that Act), such material would be subject to the Act's amendment process, to the extent that the material was not exempt; see SORN FHFB-6.

Section 8.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

See response to question 2.2 above.

8.2 Will Finance Board contractors have access to the system?

Yes, if access is approved by the Inspector General or designee.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All Finance Board employees complete annual Privacy Awareness training and contractors sign confidentiality statements.

8.4 What technical safeguards are in place to protect the data?

See response to question 2.2.

8.5 What auditing measures are in place to protect the data?

As soon as projects are completed, the projects are "finalized" where all data is write protected, which is performed by the TeamMate Administrator. In addition, any documents containing PII are protected by designating as "Confidential" in TeamMate, where only those with the same role level or higher can access the file. This will be performed by the TeamMate Administrator, who will designate only the IG has having the same role level (Administrator), which would preclude anyone but the IG and TeamMate Administrator from accessing the file.

As soon as contract employees complete their audits on TeamMate, they are removed from the GSS system, which would prevent them from accessing the TeamMate project files that are stored on the O drive of the agency LAN system (GSS). Although some contractors may download TeamMate files to store at their offices (such as onto CDs), the files are automatically encrypted and the contractor must use a password to open the files later. Confidentiality Agreements are signed at contract inception with the contractors working with the OIG. These Confidentiality Agreements require the return of unneeded Confidential Data to the IG or the Audit Director or notification to either of them about the destruction of such Data. "[U]nneeded" and "Confidential Information" are defined in the Confidentiality Agreements; the definition of Confidential Information is broad enough to include PII.

Any hard copies of PII-type records would be stored in locked file cabinets in the OIG area. Additionally, the OIG AOM provides brochures to each contractor that works at the OIG office indicating that all PII-related information in hard copies will be locked in their file cabinets if they leave the OIG area.

8.6 Has Certification & Accreditation been completed for the system or systems supporting the program?

No.

Signature Page

Jay D. Jacobsen 2/12/08

Jay D. Jacobsen, TeamMate System Owner

Federal Housing Finance Board

N/A – Commercial Software Package

System Developer
Federal Housing Finance Board

D Reed 2/12/2008

Information Security Officer
Federal Housing Finance Board

Thomas Khan 2/13/2008

Chief Information Officer
Federal Housing Finance Board

2/13/08

Chief Privacy Officer
Federal Housing Finance Board