# Privacy Impact Assessment

For

# TeamMate Audit Management System (TeamMate)

Date:
July 9, 2014

Point of Contact:

**Hui Yang**

Hui.Yang@ed.gov

System Owner:

**Wanda Scott**

Wanda.Scott@ed.gov

Author:

**Mike Burgenger**

**Office of the Inspector General (OIG)**
**U.S. Department of Education**

**1. System Information.**

*Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.*

The TeamMate Audit Management System (TeamMate) is a commercial off-the shelf software application produced by Wolters Kluwer Financial Services (WKFS) designed to control audit planning, fieldwork, collaboration, review, reporting, resolution, follow-up, and efficiency.

Data entered into TeamMate is captured in a centralized database managed by OIG. TeamMate data is accessible over the ED intranet using OIG's Citrix desktop or the client application on a government computer.

TeamMate is OIG's database for electronic audit, inspection, and quality control review project files. We manage TeamMate data in accordance with Federal retention requirements.

**2. Legal Authority.**

*Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?*

5 U.S.C. Appendix § 4(a) and 6(a) (Inspector General Act of 1978) authorizes the Inspector General to conduct, supervise, and coordinate audits relating to the programs and operations of the Department and to have access to all documents or other material available to the Department which relate to its programs and operations.

**3. Characterization of the Information.**

*What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?*

The nature and amount of PII collected and maintained varies by the objective and topic of the audit. For instance, an audit examining the timing and appropriateness of student loan payments to Federal Student Aid recipients will often contain student names, home addresses, email addresses, social security numbers, financial transactions, educational achievement data, dates of birth, income information, and other PII needed to address the audit objective. Conversely, an audit examining a school improvement grant might not contain any PII.

PII-based audit evidence usually comes from a database, electronic file or hard copy record collected from an Institution of Higher Education, State Educational Agency (SEA), Local Educational Agency (LEA), Private Lending Institution, or the U.S. Department of Education. Any PII added to a TeamMate project is contained solely in the TeamMate database but might be independently verified against ED databases.

TeamMate captures OIG employee time, effort, and expense information related to OIG audit projects in the Time and Expense Capture (TEC) module of the application. User information includes the employee's grade, rate of pay, location, ED email address, ED login id, ED employee id, ED phone

number, qualifications, and work address. Employee data is input every month by employees, or imported into the system from other ED personnel databases.

**4. Why is the information collected?**

*How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.*

PII is obtained to conduct, supervise, and coordinate audits relating to Department programs and operations as required by the IG Act. Our audit objectives frequently require that we examine whether recipients of Federal funds complied with expenditure, use, and disbursement requirements. We collect PII during the conduct of audits primarily where individual records are tracked using PII data as a unique identifier (like a social security number). In cases where the funds are disbursed to individual higher-education students, we must collect SSNs to match recipient records against the corresponding record in ED systems. Collecting PII is critical to our audit work in any case where a review of individual-level data is required by the audit objective.

The risk of unauthorized access to PII is mitigated by using multiple information system controls. The TeamMate database can only be accessed from ED computer systems, which includes OIG-issued notebook computers, OIG servers, and the OIG Citrix desktop. A user must be initially authenticated on the ED network and again on the TeamMate database to gain access. A user is only given sufficient access to the database to accomplish their work. A user must have the TeamMate desktop software, connection file, and be authenticated by the database to gain access from an OIG computer. Once connected to the database, a user can work in the database or create a copy of the project to work offline on their OIG computer. Files on OIG computers are protected by FIPS 140-1 compliant whole disk encryption and endpoint software. Additionally, TeamMate project files are individually encrypted apart from the whole disk system.

Server access to the TeamMate database is limited to authenticated system personnel with an operational need and sufficient clearance. Access to the server is only available on the ED intranet from ED computer systems.

**5. Social Security Number (SSN).**

*If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.*

TeamMate does not collect SSNs directly from individuals, but rather stores SSNs received from the institutions and entities we audit. When our audit objectives require us to evaluate compliance with Federal requirements at the student level, such as audits of a school's administration of federal student aid programs, we use SSNs to compare student financial aid records received from an auditee with records in ED systems. Our use of SSNs is solely intended to determine compliance with Federal requirements consistent with our objectives. While we try to limit the collection of SSNs whenever we can, it is impossible to avoid collecting them as long as the information systems we audit continue to use them for identification purposes or program compliance. TeamMate does not retrieve information about

individuals using an SSN. PII is stored in individual Acrobat, Word, or Excel work papers in a TeamMate project and is not in searchable database fields.

SSNs are often the only unique identifier that allows OIG auditors to positively identify individuals especially during audits of federal student aid involving financial transactions. There is no feasible alternative to using SSNs since Department record systems use SSNs to disburse federal student aid funds. In elementary and secondary education audits, we often use unique student identifiers instead of SSNs because many younger students do not possess a SSN making a separate identifier more accurate and preferable.

**6. Uses of the Information.**

*What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.*

TeamMate data is used to support findings and recommendations reached during and reported in our audit reports and other products. External and internal reviewers use TeamMate data during quality assurance reviews to monitor OIG compliance with government audit standards. We also use staff resource and milestone information collected in TeamMate to assess the efficiency and performance of the OIG organization, field offices, and employees.

TeamMate collects information in a commercial off the shelf (COTS) enterprise database application that provides built-in analysis and reporting options. Customizable reporting and analysis options are also available in the database application to authorized users.

TeamMate projects are a reflection of the type of audit performed. Thus, the audit projects often blend a combination of publicly available information, proprietary business data, personally identifiable data, and internal ED data. We often use student data that is summarized at the school, district, state, and sometimes national level to support conclusions reached in the conduct of our audits. In cases where we can use individual-level information that is NOT personally identifiable, we make every effort to do so. Our goal is to collect sufficient data in the system to support our audit findings and recommendations, but not excess data.

**7. Internal Sharing and Disclosure.**

*With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?*

TeamMate data is considered the work product of OIG auditors and is only shared internally with staff within ED with a need to know the information in the performance of job duties. When sharing TeamMate data with ED offices, only information specific to the audit and function in question is exported to a secure file and provided to ED staff responsible for audit resolution.

**8. External Sharing and Disclosure.**

*With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?*

TeamMate data is shared with external users for purposes of required peer review in accordance with generally accepted government auditing standards (GAGAS) issued by the Government Accountability Office (GAO), the Council of Inspectors General on Integrity and Efficiency (CIGIE), and other standard setting organizations.

Generally, TeamMate data is not shared externally other than with other OIGs for the purpose of conducting peer reviews or with auditees for the purpose of audit resolution. Staff from other OIGs conducting the peer review must sign a non-disclosure agreement before they are given access to data. When required to share TeamMate data, OIG policy requires the minimum amount of data be shared to fulfill the requestor's purpose. Data is only shared externally for specific projects and only with those with a need or legal right to know and either in hard copy or encrypted media.

TeamMate provides an offline viewer that allows a 3rd Party without a license to the TeamMate software to open projects in a read-only manner. The viewer gives OIG the ability to make specific documents available from a TeamMate project without providing full access to all documentation. The offline project is protected by a username and password. The TeamMate project data can be safely encrypted to FIPS 140-1 standards (when required) and sent to a 3rd party by commercial carrier. If data contains protected PII, OIG will limit access to the data to ED-issued encrypted laptops in ED offices.

OIG may share information contained in TeamMate pursuant to the routine uses listed in the Privacy Act System of Records Notices (SORNs) for the Non-Federal Auditor Referral, Debarment, and Suspension files (18-10-03). Information may be shared with external entities without the consent of the individual if the routine use disclosure is compatible with the purposes for which the record was originally collected. Specific disclosures may include the following:

- Federal, state, local or foreign agencies or law enforcement or oversight agencies
- Public or private entities when necessary to obtain other information
- Litigation and alternative dispute resolution
- Contractors and consultants
- Debarment and suspension
- Department of Justice advice
- Member of Congress
- Benefit program
- Collection of debts and overpayments
- Council of Inspectors General on Integrity and Efficiency.

**9. Notice.**

*Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?*

OIG does not collect PII directly from individuals during audits and therefore does not provide a privacy notice to individuals about whom it collects PII. During quality control reviews of Non-Federal auditors, we sometimes collect PII related to referrals, suspension, and debarment of auditors and audit firms, which is covered under SORN 18-10-03.

**10. Web Addresses.**

*List the web addresses (known or planned) that have a Privacy Notice.*

https://www2.ed.gov/about/offices/list/oig/hotline.html
https://www2.ed.gov/about/offices/list/oig/warning.html

**11. Security.**

*What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?*

Specifically within the TeamMate application, we protect any work papers containing PII data with TeamMate's confidential control. The confidential control limits access to the PII data to users with privileged access to the project and prevents "read-only" users from gaining access to the information. This occurs after the user has been authenticated on the ED network, provided access on the TeamMate application, and given rights to the individual project within the database.

We also employ general policy and procedure safeguards to protect TeamMate data. For example, all government employees and contractors must have an ED account to gain access to TeamMate. TeamMate system user access is granted based on a need-to-know basis and the least allowable privilege needed to perform required duties. All information in TeamMate is controlled through network controls, user permissions, user authentication, and database access controls. ED employs firewalls, host-based and network based Intrusion Detection/Prevention Systems (IDS/IPS), and antivirus software that notify security officers and key ED administrators of incidents. TeamMate relies on ED and the General Support Systems (GSS) to monitor physical access to the information system and to respond to physical security incidents. The OIG servers that run TeamMate are housed in segregated OIG racks. Access is controlled 100 percent with the racks and perimeter fencing around the OIG section of the datacenters. An email alert and video surveillance system is used to monitor the OIG servers. The datacenters housing TeamMate servers require photo-identification and access permissions from management to enter the buildings. The critical servers and routers are housed in secure areas that are accessible only to authorized and badged personnel with keycard entry.

TeamMate is scheduled to undergo a security scan and audit in May 2014 with the goal of securing an Authentication to Operate (ATO) for the entire TeamMate suite no later than 1 October 2014.

**12. Privacy Act System of Records.**

*Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?*

No, PII cannot be retrieved by an identifier because the information is not indexed or referenced based on unique or identifiable information. PII may be present in the audit and/or inspection supporting documentation, but is not the primary data in the system.

In accordance with 5 U.S.C. § 552a(e)(4) and (11), OIG published a SORN covering certain information contained in TeamMate related to review of Non-Federal Auditors. SORN 18-10-03, covering Non-Federal Auditor Referral, Suspension, and Debarment files, is located at 64 FR 30155 and is updated at 64 FR 72406-72407.

**13. Records Retention and Disposition.**

*Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:*

Data retention is managed in accordance with the ED Records Schedule based upon NARA retention standard N1-441-02-1. ED Records Schedule #216 approved on 06/05/2002 covers disposition of OIG audit, investigative analysis, inspection, and other records.