U.S. Securities and Exchange Commission

TeamMate Plus
PRIVACY IMPACT ASSESSMENT (PIA)

March 22, 2023

Office of Inspector General

Privacy Impact Assessment

TeamMate Plus Software v26.0.15.0

Section 1: System Overview

1.1 Name of Project or System

TeamMate Plus v.26.0.15.0

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Inspector General (OIG)

☐ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 8/20/2015

Last updated: 7/19/2018

Description of update: Upgrade Teammate Plus from version 24.0.492.0 to version 26.0.15.0 to provide support for Microsoft Structured Query Language (SQL) Server.

1.4 Does the system or program employ any of the following technologies?

☐ Enterprise Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☐ Web Portal

☒ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The SEC Office of Inspector General (OIG), Office of Audits, uses TeamMate Plus, Commercial of the Shelf (COTS) product, to automate the workflow of audit-related working papers. The TeamMate Plus application suite provides OIG auditors the following capabilities:

- Identify, schedule, document, report and track time and expenses for audits
- Standardize OIG's process of creating audit records
- Develop and store audit work papers and reports
- Provide remote access to audit information
- Track audit reports and recommendations

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Inspector General Act of 1978, as amended, Pub. L. 95-452, 5 U.S.C. App 3.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☐ No

☒ Yes

If yes, provide the purpose of collection:	The collection of SSN data is a collateral submission of data. However, SSN data may be included in supporting documentation from data gathering and evidence as authorized by the Inspector General Act of 1978, as amended.
If yes, provide the legal authority:	

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN
SEC-18 Office of Inspector General Working Files

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No
☐ Yes

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The primary privacy risks are that personal information may be collected without clear purpose or the information provided for one purpose may be used inappropriately. The risks are mitigated by clearly stating the authorized purpose for the collection in System of Records Notice (SORN) SEC-18, limiting the information collected to only what is authorized and using collected information in accordance with the routine uses identified in the SORN.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☒ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☒ Financial Transactions
☒ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☒ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data

☒ Name	☒ Date of Birth	☐ Marriage Records
☐ Maiden Name	☒ Place of Birth	☒ Financial Information
☐ Alias	☒ Home Address	☐ Medical Information
☒ Gender	☒ Telephone Number	☐ Military Service
☒ Age	☒ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☒ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	
☐ Other:		

Work-Related Data

☒ Occupation	☒ Telephone Number	☒ Salary
☒ Job Title	☒ Email Address	☒ Work History
☒ Work Address	☐ Certificate/License Number	☐ Business Associates

☒ PIV Card Information	☐ Fax Number	
☐ Other:		
Distinguishing Features/Biometrics		
☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		
System Administration/Audit Data		
☒ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☒ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other:		

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

PII is collected, used, shared, and maintained to support audit report development.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Purpose: System Administration/Audit Data, PIV Card, and Employee ID information identified in section 3.1 above is collected in support of audit report development.

☒ SEC Federal Contractors
Purpose: System Administration/Audit Data information identified in section 3.1 above is collected in support of audit report development.

☒ Interns
Purpose: System Administration/Audit Data information identified in section 3.1 above is collected in support of audit report development.

☒ Members of the Public
Purpose: Provided to OIG as part of audit specific documents/data, "as collected" by "other" SEC systems.

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: Information is collected in support of audit report development.

☐ Job Applicants
Purpose:

☒ Vendors
Purpose: OIG may request vendor technology or trade secret data in support of method, validity or technical best practice. Subject matter expert data is collected in support of audit report development.

☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

OIG only collects information, including PII, which is necessary to support audit conclusions. PII is redacted from audit findings prior to audit report review by the Commission. Actual data, including PII, is not used for testing, training, or research.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes.

DAA-0266-2018-0002 "Office of Inspector General Records"

3.6 What are the procedures for identification and disposition at the end of the retention period?

Records are maintained until they become inactive, at which time they will be retired or destroyed in accordance with DAA-0266-2018-0002. Work paper records are maintained for 10 years and final reports are maintained indefinitely.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

Given the type of information collected, the primary privacy risk is inadvertent or unauthorized disclosure of PII. This risk is mitigated through the use of identification and authentication mechanisms and role-based access control to restrict access to information in TeamMate Plus to only authorized users.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☐ Privacy Act Statement

☒ System of Records Notice
SEC-18 "Office of Inspector General Working Files"

☐ Privacy Impact Assessment
Date of Last Update:

☐ Web Privacy Policy

☐ Other notice:

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The primary privacy risk is inadequate notice. This risk is mitigated because SORN SEC-18 provides the authority for collecting information and identifies routine uses of information collected.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

The TeamMate Plus tool is used to interact with data as part of the audit workflow process. Data analysis does not occur via tool, as the tool is only a workflow environment for the audit process.

5.2 Will internal organizations have access to the data?

☒ No
☐ Yes
Organizations:

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The privacy risk from internal sharing is unauthorized or inadvertent disclosure of nonpublic information to individuals without a need-to-know. This risk is mitigated because TeamMate Plus is only available to authorized SEC OIG users who are approved for access by the Business Owner (BO) and assigned specific user roles.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes
Organizations:

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

There is no risk to privacy from external sharing because PII is not shared with external organizations.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☐ Directly from the individual.
☒ Other source(s): Information is collected from individuals with pertinent knowledge of an OIG inquiry, and SEC emails, documents and files.

6.2 What methods will be used to collect the data?

The data collected is obtained from individuals in electronic and hard copy form. Electronic data may be scanned, upload from email or shared drives. Data exists on SEC storage and thus can be made available to the OIG by copy/transfer to storage accessible to OIG. OIG staff manually enter information or scan documents into TeamMate Plus. Information from emails and shared SEC drives from other SEC offices/divisions is scanned or uploaded from e-mail/shared drive into TeamMate Plus.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

OIG audit staff use electronic and other verification services, such as the Federal Bureau of Investigation (FBI)-provided National Instant Criminal Background Check System (NICS), to verify information for accuracy and completeness.

6.4 Does the project or system process, or access, PII in any other SEC system?

☐ No
☒ Yes.
System(s): TeamMate Plus integrates with Active Directory for authentication and to import user information (excluding passwords).

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The primary privacy risk is inaccurate or outdated information. This risk is minimized as information is collected directly from the individual from sources outside of TeamMate Plus, as discussed in section 6.2, and verified through external information services as discussed in section 6.4.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

No opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project. The OIG, per the Inspector General Act, has the authority to collect information in the performance of its duties.

7.2 What procedures are in place to allow individuals to access their information?

Individuals wishing to obtain information on the procedures for accessing information about themselves in the system may contact the Freedom of Information Act (FOIA)/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit a request online. However, individuals cannot access information about themselves that is part of investigatory materials compiled for law enforcement purposes.

7.3 Can individuals amend information about themselves in the system? If so, how?

Individuals cannot amend information about themselves that is part of investigatory materials compiled for law enforcement purposes.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

Individuals are not generally permitted to access or correct available records about themselves in Teammate Plus. There is risk that inaccurate or erroneous information about an individual could be stored in the system. The risk is minimized because information is checked for accuracy and completeness as discussed in section 6.3. Investigatory information compiled for law enforcement purposes is exempt from Privacy Act provisions.

Section 8: Security

8.1 Does the project or system involve an online collection of personal data?

☒ No
☐ Yes

Public
URL:

8.2 Does the site have a posted privacy notice?

☒ No
☐ Yes
☐ N/A

8.3 Does the project or system use web measurement and/or customization technologies?

☒ No
☐ Yes, but they do not collect PII
☐ Yes, and they collect PII

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC staff and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

9.2 Does the system generate reports that contain information on individuals?

☒ No
☐ Yes

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☐ Yes
☒ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Unauthorized disclosure is a residual risk related to access to information in TeamMate Plus. This risk is minimized because access to TeamMate Plus is restricted to only authorized SEC personnel through the use of multi-factor authentication and role-based access control.