



Special Inspector General for Afghanistan Reconstruction

Main: 703-602-2500
2530 Crystal Drive
Arlington, VA 22202-3934
www.sigar.mil

PRIVACY IMPACT ASSESSMENT

INTRODUCTION

This Privacy Impact Analysis (PIA) is conducted pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347), and is used to determine the scope, justification, and appropriateness of use of information technology that collects, maintains, or disseminates information in identifiable form, also referred to as personally identifiable information (PII).

Directorate or Component:	Audit
System Name:	TeamMate, Audit Document Management System
System Acronym:	TeamMate
System Owner:	Office of Inspector General

A. Information and Privacy

To fulfill the Special Inspector General for Afghanistan Reconstruction's (SIGAR) legal obligations to protect PII, SIGAR systems must meet the following requirements:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, both inside and outside SIGAR, to share sensitive personal information.

B. Contact Information:

1. Who is the person completing this PIA?

Name: Larry Dare
Title: Senior Auditor
Component: Audit: Quality Control
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA, 22202

2. Who is the System Manager for this system or application?

Name: Larry Dare
Title: Senior Auditor
Component: Audit: Quality Control
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA, 22202

3. Who is the IT Security Manager for this system or application?

Name: Roland Wong
Title: IT Director
Component: Information Management Office
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA, 22202

4. Who is the Chief Privacy Officer or designee who reviewed this document?

Name: Hugo Teufel
Title: Director, Privacy, Records, & Disclosure
Component: OGC/PRD
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA, 22202

C. System Description

This section of the PIA describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

Overview of the TeamMate Application: The TeamMate application is a commercial off-the-shelf information system supporting SIGAR's audit/evaluation responsibilities established by the Inspector General Act of 1978. The system is maintained to increase the efficiency and productivity of the audit/evaluation process by automating working paper preparation, internal review, and retention. The system utilizes the commercial software product, TeamMate, to manage and integrate working papers prepared with various standard office automation products.

D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

The system is used in conducting audit/evaluation work of the Special Inspector General for Afghanistan Reconstruction's audit responsibilities and in preparing related reports on behalf of SIGAR. Such work enables SIGAR to fulfill its responsibilities under the Inspector General's Act. TeamMate automates documenting SIGAR's audit work – planning, preparing, reviewing, and storing – in an electronic format. Although personally identifiable information is typically not included in this system, the nature and scope of any such information could include the following:

- social security number,
- banking information,
- full name,
- street address,
- date of birth,
- e-mail address,
- telephone number,
- photographs,
- employee disciplinary data,
- passport data,
- education,
- criminal history, and
- employment history.

The specific nature and scope of such information would be determined by the objectives of the audit/evaluation to which it relates. Furthermore, the

nature of any personally identifiable information would vary depending on the circumstances of the audit/evaluation. To the extent that personally identifiable information is collected, it is generally maintained in the audit/evaluation work papers and not disseminated to the public or readers of the related reports.

2. Can individuals “opt-out” by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

No The TeamMate system will be used to deposit and store information necessary to do audit work and SIGAR employees or others are required to cooperate with IG activities. Although personally identifiable information is typically not collected in the course of an audit or evaluation, if such information were collected, it would be collected only to the extent necessary to meet the objectives of the assignment to which it relates. The individual, nevertheless, would not have the right to consent only to a particular use as such a limitation may be incompatible with SIGAR’s legal responsibilities. To obtain access to the system, and use it as intended, a certain amount of PII will likely be necessary.

3. What are the sources of the information in the system? How are they derived? Explain.

Data in the system consists of documents and data requested from, and the results of discussions with, military, State, USAID, and non-governmental sources. Information in the system is derived from discussions with federal and non federal sources as well as analyses done by SIGAR employees, contractors, and other staff. SIGAR has a statutory right to federal information and statutory authority to subpoena records from non-federal entities.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

Department of State, Department of Defense, and United States Agency for International Development, their representatives, and private contractors that work for them, may have a need on a case-by-case basis to review audits/reviews conducted using TeamMate. Other law enforcement agencies may be provided the information based on the scope and findings of an audit/review; information may also be shared with auditees and other third parties when necessary to obtain information relevant to the audit/review. The SIGAR's audit/review process is subject to a quality control review conducted by the Inspector General of another agency.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

None.

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

DOS, DOD, and USAID contractors. Also see number 4.

E. Access to Data:

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

Auditors working on assignments will have access in order to record the results of their work and identify reportable issues. Managers will review auditor's work, and system administrators will have access in order to maintain and trouble shoot system problems. Access can be controlled by the system administrator and only those that have a need are given rights to view the data.

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

SIGAR is currently working on access procedures and approval process. The system is not yet procured and this is not yet an issue. However,

access is role based according to job function and contingent on a official need to know.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

There will be restrictions on user access to data that does not pertain to the assignments they are working on. Generally, users will have limited access to the system which allows them to see only the information specific to the audit they are working on. Certain supervisory personnel will have broader access rights.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

TeamMate log all access to individual project which includes date and time of access. Other controls that prevent the misuse of data by those having access to the data; including, passwords, user identification, network permissions, and software controls. Additionally, TeamMate users are required to complete SIGAR security awareness training on an annual basis.

5. Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.

No.

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

N/A. The public or others outside SIGAR will not have access to the system.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

N/A. Other agencies will not have access.

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

Individual auditor in charge (AIC) will be responsible for the individual audit project and the documentation. The TeamMate system administrator will be responsible for the system integrity. The database administrator and network security administrator will be responsible for the overall database and network security of the TeamMate system.

9. Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the agency be affected?

Because the TeamMate system only uses limited privacy-related information, the impact of a disclosure of information is minimal. The system may contain sensitive information that should not be disclosed to persons outside SIGAR.

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

We are purchasing a COTS system. A contractor designed the system, will provide enhancement and security updates, and maintain the system. Contractor has not yet signed a Contractor Confidentiality Agreement.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

N/A

F. Accuracy, Timeliness, and Reliability

1. How is the data collected from sources other than SIGAR records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.

N/A

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

N/A

G. Attributes of the Data?

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

The information collected in TeamMate is relevant and necessary to support the functional requirements on the application. Its use is part of the system design and is documented in the system documentation provided by the system's manufacturer.

2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

The TeamMate application is not intended to, nor is it programmed to, determine whether personally identifiable information can be derived through the aggregation of information collected. Users, through reviewing the collected information, would have to make this determination. The determination would be based on the judgement of the user.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

The TeamMate application is not intended to, nor is it programmed to, determine whether personally identifiable information can be derived through the aggregation of information collected. SIGAR assignment team members, through reviewing the collected information, would have to make this determination. The determination would be based on the judgement of the assignment team members.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

See section E, Access to Data, for the controls on access to a TeamMate file and data.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

TeamMate offers limited search and retrieve capabilities. Full text searching is available on any text field of a TeamMate form based on a word or phrase. TeamMate does not allow text searches over numerous individual workpapers and does not provide for the retrieval of information using any type of personal identifier.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

No reports are produced about individuals.

H. Maintenance and Administrative Controls:

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? Will the same controls be used? Explain.

N/A. We anticipate that the TeamMate application will be operated at only one site, and will amend this PIA if otherwise.

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

SIGAR will retain audit documentation in the TeamMate system until all audit recommendations are closed. At that time, records will be transferred to Federal Records Center and maintained in accordance with SIGAR's Audit Record Retention requirements. SIGAR's Record Retention schedule is approved by the Archivist of the United State to provide disposition authority for records unique to SIGAR.

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

Audit records will be retained, disposed, and transferred to the National Archives in accordance with the SIGAR Audit proposed records schedule. The proposed dispositions are a mix of temporary and permanent. Until the SIGAR records schedule is signed by the Archivist of the United States, TeamMate records will be maintained indefinitely.

4. Is the system using technologies in ways that the agency has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

N/A.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

The use of TeamMate should have no affect on privacy. Any privacy related information is included in the system only if relevant to the objectives of an audit. Any privacy related information in reports or related documents would not, in general, be publically released. Moreover, personally related information cannot be retrieved from the system by personal identifier.

The use of this technology does not include the risk of compromising the integrity of privacy related information in the system when compared to information maintained in hardcopy files. In fact, the use of TeamMate may reduce the risk of compromise in that paper records may be easier to review than a series of computer screens.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

There is no monitoring of individuals.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

The system is not used to monitor individuals. The system is only accessible by those SIGAR employees who have been authorized and then only for selected information on a need to know basis.

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

SIGAR-05 Audit Records.

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No.

I. Business Processes and Technology

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

No.

2. Does the completion of this PIA potentially result in technology changes?

We are not aware if the manufacturer of TeamMate is contemplating any changes to their product based on sensitive information issues.

**Privacy Impact Assessment
Authorization Memorandum**

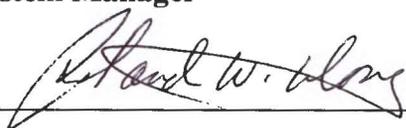
This system or application was assessed and its Privacy Impact Assessment approved for publication.



System Manager

07/19/2012

Date



Information Technology Security Manager

07/23/2012

Date


(acting)

Chief Privacy Officer

7/19/2012

Date