Special Inspector General for Afghanistan Reconstruction
Main: 703-545-6000
1550 Crystal Drive, 9th Floor
Arlington, VA
www.sigar.mil

John F. Sopko, Special Inspector General

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 - Forensics**
System Name:	**Forensic Contract Universe Database**
System Acronym:	**N/A**
System Owner:	**Forensic Team**

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.

B. Contact Information:

1. Who is the person completing this PIA?

   Name: Holly Roller
   Title: Director of Forensic Audit
   Component: Audits

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

   Name: Holly Roller
   Title: Director of Forensic Audit
   Component: Audits

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

   Name: Roland Wong
   Title: IT Director
   Organization: IMO

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

   Name: Hugo Teufel
   Title: Director, Privacy, Records, and Disclosure
   Component: OGC/PRD

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.

The database contains many different files consisting of all the appropriation, obligation and disbursement data related to the Afghanistan reconstruction effort. Databases include disbursement information down to the contract level, including contractor name, contract number, appropriation/obligation/disbursement amount(s), contract information (sole source/competitively awarded, contract award date, contract type, contracting office), description of product/services, applicable program, sector, and/or subsector. Data also includes Foreign Military Sales (FMS) transactions which include case and country code information, executing office, and quantity of items purchased.

Data is collected from various agencies including the Department of Defense (DoD) Defense Finance and Accounting Service (DFAS), Defense Security Cooperation Agency (DSCA), Department of State (DoS) and United States Agency for International Development (USAID). Data is collected from Excel spreadsheets, Access databases, .csv files, and various websites including the Federal Procurement Database System (FPDS) and the Centralized Contractor Repository (CCR.gov). The data is then uploaded to an access database, where reports are created off the data to provide overall insight into where dollars are being spent on the reconstruction effort, to whom, and for what products and services.

The data will be utilized initially by audit and investigative directorates within SIGAR in order to obtain information on specific contracts and contractors. The database will reside on the Audit shared drive.

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.

   Name (if the payee for a "contract" is an employee, e.g. for expense reimbursement); contract number, and if available; and contracting officer's name.

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 Explain: Vendors and other entities provide information to contracting organizations when a contract is awarded. This data is fed directly from agency disbursement systems, and is analyzed by SIGAR forensic staff.

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

   Data is collected from various agencies including DoD – DFAS, the DSCA, State, and USAID (procurement and disbursing systems), as well as public websites including the Federal Procurement Database System (FPDS) and the System for Award Management (sam.gov) formerly

Centralized Contractor Registration. Data is collected and stored in excel spreadsheets, access databases, .csv files, and CD/DVD format.

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.

   DoD, DSCA, State, USAID. The data is used to provide detailed information to audit and investigative teams with respect to specific contracts and/or contractors.

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.

   N/A

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.

   N/A

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.

   Audit and forensic staff will have access to the data. The data files are located on the secure Audit shared drive. Data is intended to be utilized for both forensic and audit work.

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.

   Access to the audit shared drive is determined by user roles. Users who work on audits, along with support staff, are granted read only access to the data. Users who do not meet these criteria may not access the data.

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

Data input and manipulation will be limited to the forensic team only. Access to the database and related reports will be available to the SIGAR organization via the shared drive.

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.

   All data is unclassified and access to this data is unrestricted to SIGAR employees as part of SIGAR's mandate. Only authorized users are granted access to the data in the system. Furthermore, access to SIGAR's files is limited through use of Department of the Army's common access card (CAC) system, which provides two factor authentication security.

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.

   This data is currently restricted to the SIGAR organization, whose congressional mandate allows employees to access all information and data related to Afghanistan reconstruction. The only "private" information that is stored in this database is contractor name, which may be an agency's employee name if the payment was for a reimbursement. This information is unclassified.

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

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.

   All data is unclassified information; access to the audit shared drive is determined by user roles. Users who work on audits, along with support staff, are granted read ony access to the data. Users who do not meet these criteria may not access the data.

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

   The only "private" information that is stored in this database is contractor name, which may be an agency's employee name if the payment was for a reimbursement. This information is unclassified.

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?

    There is no contractor involvement with the exception of IT contractors that may support management of the SIGAR shared drive and related systems.

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.

    No other agencies are granted access to the SIGAR internal shared drive.

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.

   Data is reconciled to previous feeds received from the agency and/or quarterly report numbers. There is no verification of the various agencies' data feeds. Data is received either on a password-protected CD/DVD, through email, or via an ftp site from other agencies; network scans documentation for viruses upon downloading/opening.

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.

   Dollars are reconciled against reporting receiving by Quarterly Reporting team; completeness has been an ongoing issue and all data has not been verified as complete. Forensic team has worked with the data available thus far. Other data characteristics are reconciled as well (such as the use of country code and case data for DoD related data).

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.

   Yes, all data being collected and stored within the database is being used for providing disbursement, appropriation, obligation, contract, and contractor information for the purposes of audit and investigative research and planning, as well as providing overall statistics for reporting purposes. Descriptions of data fields, tables, and reports have been documented in a user guide, which is currently in progress, and stored with the database on the shared drive within an excel file.

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.

   No.

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

   No.

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.

   No; consolidation of data does not result in other personal identifiable information. Access to update data will be restricted through Access database controls to team members responsible for updating the database. Access to run reports off of the database is unrestricted to SIGAR personnel on the audit shared drive. Access to the audit shared drive is determined by user roles. Users who work on audits, along with support staff, are granted read only access to the data. Users who do not meet these criteria may not access the 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.

Data is retrieved by opening tables within the database or running reports created within the database. Reports are run off of particular characteristics such as contractor name, contract number, implementing agency, or reconstruction sector. Personal identification information is not within the database.

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.

   None – the only unique individual information may be if an employee's name is listed as the payee for a vendor payment. Reports can be run off of contractor name; access is restricted to SIGAR organization where it resides on the shared drive.

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.

   Data resides in one site, on SIGAR's S:/ drive. Users may access the data from terminal computers, but cannot change the user access configuration from these computers.

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 submitted a records retention schedule to the National Archives and Records Administration, which included disposition periods for Audit records. The tentative retention periods for the data in this system are as follows: Work Files- Temporary, close after final resolution of audit findings. Destroy 7 years after file closure. Final Reports- Permanent, cutoff at 3 years after final resolution of audit findings. Transfer to the National Archives 10 years after cutoff, or at the end of the agency.

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.

   Final Reports- Permanent, cutoff at 3 years after final resolution of audit findings. Transfer to the National Archives 10 years after cutoff, or at the end of the agency. The data will be removed from the system and

degaussed. The owner of the system will document the destruction through the agency's Electronic Records Management System.

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

   No.

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.

   N/A

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.

   N/A

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

   Same controls utilized by IT department to restrict shared drive access.

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 – reports would just be developed off the databases.

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?

   No.

Privacy Impact Assessment
Authorization Memorandum

This Privacy Impact Assessment is approved for publication.

K. A. Taipale
for Holly Roller

System Manager — **Date** 7/29/2012

Richard W. Hove

Information Technology Security Manager — **Date** 7/31/2012

Kate Gasztonyi (acting)

Chief Privacy Officer — **Date** 7/20/2012