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:	**Management & Support**
System Name:	**Inventory Database System**[1]
System Acronym:	**IDBS**
System Owner:	**SIGAR**

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.

[1] IDBS was originally designed as a component program of an intended repository for SIGAR's web applications, known as SIGAR Knowledge Online (SKO). IDBS was the only application developed under the SKO concept before that project was cancelled. IDBS is currently known as SKO by Army's Information Technology Agency (ITA), and in IDBS' Tenant Security Plan the system is known as SKO.

B. Contact Information:

1. Who is the person completing this PIA?

Name:	Patrick Peterson
Title:	Project Management Officer
Component:	Project Management Office, Management and Support
Address:	1550 Crystal Drive, Suite 9000, Arlington, VA 22202

Name:	Rushad D. Bharucha
Title:	Project Manager
Component:	Project Management Office, Management and Support
Address:	1550 Crystal Drive, Suite 9000, Arlington, VA 22202

2. Who are the System Managers for this system or application?

Name:	Sy Chen
Title:	Lead Application Developer
Component:	Applications Development, Management and Support
Address:	1550 Crystal Drive, Suite 9000, Arlington, VA 22202

Name:	Sharon Wong
Title:	Application Developer
Component:	Applications Development, Management and Support
Address:	1550 Crystal Drive, Suite 9000, Arlington, VA 22202

Name:	Marcus Boddie
Title:	Logistics Specialist and Property Book Officer
Component:	Business Operations, Management and Support
Address:	1550 Crystal Drive, Suite 9000, Arlington, VA 22202

3. Who is the Information System Security Officer for this system or application?

Name:	Roland Wong
Title:	IT Director
Component:	Information Management Office, Management and Support
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

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 Inventory Database System (IDBS), developed in-house and using Microsoft .NET as its framework, is a web-based inventory management application that contains information on key SIGAR equipment assigned to staff in both Washington and Afghanistan. IDBS tracks equipment that directly affects SIGAR operations and assignments, including firearms, ammunition, and other sensitive and non-sensitive items. IDBS improves SIGAR's ability to efficiently manage its resources, and ensures that key equipment is accounted for.

Apart from the personal information needed to created accounts and allow user login, IDBS contains the following information:

- Personal:
  - Staff members' names.
  - CAC numbers.
  - Email addresses.
  - Duty locations (either Afghanistan or DC).
  - Work and/or mobile phone numbers.
- Inventory:
  - Listings of equipment assigned to the SIGAR Investigations Directorate, including the item name, manufacturer, type of equipment, and serial number.[2]
  - Locations of where the equipment is located (either in Washington or Afghanistan).
  - Person to whom the item is assigned.
  - The PBO can use the note field in the equipment description to list previous recipients of a given item, for usage tracking purposes.

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.

[2] IDBS currently only contains Investigations equipment, but a future version of this project will include equipment from other Directorates.

To grant user access rights, IDBS uses Common Access Card (CAC) authentication. Data stored on a user's CAC includes his/her name, Work Location (i.e. DC or Afghanistan), CAC Number, and E-mail Address. However, IDBS requires that only a user's CAC number (and PIN) and e-mail address be passed to the system during authentication.

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: SIGAR employees receiving SIGAR property must use IDBS, which requires CAC authentication to gain access. Employees may not log in using a different method.

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

When a user attempts to access IDBS, he/she must use a computer with a CAC reader and input his/her PIN in order to gain access. Information stored on a user's CAC is passed into the system when a user attempts to login. Specifically, the authentication is processed by AKO, which checks the CAC number and PIN against a table in IDBS's database and determines if a user has been granted access to the system. Once a user has been granted access to the system, IDBS does not use CAC numbers for identification (for example, for user records). In addition, IDBS does not store a user's PIN or other sensitive data that is maintained by AKO.

Basic personnel information for users is provided by SIGAR Human Resources and the SIGAR Information Management Office (includes names, duty locations, and e-mail addresses). When this initial information is inputted during account creation, IDBS matches these criteria with CAC and email data stored on Army ITA database resources in order to generate login ability for users.

Equipment inventory records are inputted by the Super PBO, who receives this respective information from the Management & Support Directorate purchasing and/or finance staff.

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 – CAC-authentication. IDBS uses the information coded within each CAC to enable the respective user login.

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.

   None. All equipment logged in IDBS is SIGAR-owned and -operated. SIGAR will not use IDBS to track equipment on loan from other agencies (e.g. computers issued by the State Department for SIGAR personnel in Kabul).

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.

   - Property Book Officers (PBOs): PBOs are responsible for maintaining records of equipment assignment in IDBS. They have access to user records which display the equipment assigned to users. These records contain only user names; they do not have access to CAC numbers. These users must have access to this information to perform the basic functions of the system, such as assigning equipment to users.
   - Application developers: these individuals have access to user records and to the authentication tools used to grant users access to the system. These users must have access to this data because they are responsible for developing IDBS.
   - System users: All users of IDBS have access to their own record, which contains a list of equipment assigned to them. These users do not have access to any other records but their own.

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.

   All SIGAR staff members have basic access rights to the system and can view their own employee records. Property Book Officers and other officials responsible for managing inventory have access to view equipment assigned to all users. Higher levels of access are determined by employee job responsibilities and require approval by the Assistant

Inspector General for Management and Support (AIG-M&S), or his/her designee. Application developer personnel have access to data on the system but require approval from the SIGAR Assistant Inspector General of Management and Support, or designee.

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

   Restricted by level of responsibility. "Regular" users will not have access to PII other than their own work location. PBOs will only be able to determine work location and email addresses. Application Developers have full access to inputted PII to program full functionality into the system, and debug when necessary.

Privilege Level	Action	Allowed?
Read	Read Inventory	Yes
Granted to Most Users	Create Inventory	*No*
	Write in own Inventory	No
	Write in other Inventory	No
	Run Reports	No
	Open Inventory	No
	Approve Inventory	No
	Replace/Delete Approved Inventory	No
	Access own record	Yes
	Access other users' records	No
	Access own Personally-Identifiable Information (only name and location)	Yes
	Access other users' Personally-Identifiable Information	No

Privilege Level	Action	Allowed?
Create	Read Inventory	Yes
Granted to PBO	Create Inventory	Yes
	Write in own Inventory	Yes
	Write in other Inventory	No
	Run Reports	Yes
	Open Inventory	No
	Approve Inventory	No
	Replace/Delete Approved Inventory	No
	Access own record	Yes
	Access other users' records	Yes
	Access own Personally-Identifiable Information (only name and location)	Yes
	Access other users' Personally-Identifiable Information (only name and location)	Yes

Admin	Read Inventory	Yes
Granted to Super PBO	Create Inventory	Yes
	Write in own Inventory	Yes
	Write in other Inventory	Yes
	Run Reports	Yes
	Open Inventory	Yes
	Approve Inventory	Yes
	Replace/Delete Approved Inventory	Yes
	Access own record	Yes
	Access other users' records	Yes
	Access own Personally-Identifiable Information (only name and location)	Yes
	Access other users' Personally-Identifiable Information (only name and location)	Yes

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.

   New SIGAR employees receive security and information technology training as part of their in-processing, which covers user responsibilities dealing with CAC login and safeguarding of personal information.

   IDBS uses two methods to control access to PII data. First, IDBS segregates users into groups and control access to information based on a user's group. For instance, most users in IDBS do not have the ability to access user records or view equipment assigned to other users.

   SIGAR application developers are building a module to provide an auditing function that will produce reports on information that has been changed in the system. The module will monitor data in the system and, when it is altered, will identify what change was made, who made the change, and the time and date of the change. This data will be read-only accessible to application developers and the PBO and could be used to ensure data integrity.

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.

   IDBS retrieves information from the Army GAL and AKO (CAC) for user authentication.

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

   Army ITA maintains the servers and network on which IDBS resides, and is responsible for data security. The Army identifies various DoD Components when generating PIAs for its own endeavors, including, but not limited to:

   - EO 9397 (SSN) as amended;
   - DoD Directive 8500.1 Information Assurance;
   - AR 25-400-2, The Army Records Information Management System;
   - 10 USC 3013, Secretary of the Army.

   The public does not have access to the system. IDBS is only accessible on computers in which authenticated users have accessed the system via their CACs.

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?

   Other agencies will not have access to this data.

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.

   The PBO is responsible for ensuring proper use of the data. The PBO is responsible for maintaining the integrity of the data on the system and assigning users appropriate access levels based on their level of responsibility. However, the PBO is not fully accountable for all aspects of IDBS security. Army ITA maintains the servers and network on which IDBS resides, and is responsible for the security of this network. Additionally, ITA is also responsible for maintaining the security of the CAC authentication process.

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

   Because IDBS only uses limited privacy-related information (specifically, a user's CAC number, name, e-mail address, and work location), the impact of a disclosure of information is minimal. Additionally, the

database that house IDBS contain login records which Application Developers can access for auditing purposes.

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?

    N/A. Application Developers and PBOs are government employees.

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 have access or be granted access to the information within IDBS.

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.

   During login, IDBS reads an individual user's information coded on his/her CAC and the user's inputted PIN. The system checks this against PII stored on a SQL database table, across a Secure Socket Layer (SSL) connection with Army ITA. When the PIN and card information match the table information, IDBS grants the user access.

   Army ITA maintains the database and table to which IDBS conducts CAC authentication. The Army identifies various DoD Components when generating PIAs for its own endeavors, including, but not limited to:

   - EO 9397 (SSN) as amended;
   - DoD Directive 8500.1 Information Assurance;
   - AR 25-400-2, The Army Records Information Management System;
   - 10 USC 3013, Secretary of the Army.

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.

   Army/DoD produces CAC information and email addresses, from which SIGAR uses to create IDBS accounts.

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 – IDBS uses individual CAC/Outlook information in order to authenticate user login. Documented in IDBS User and PBO Manuals (attached).

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.

   Army ITA maintains the servers and network on which IDBS resides, and is responsible for data security. The Army identifies various DoD Components when generating PIAs for its own endeavors, including, but not limited to:

   - EO 9397 (SSN) as amended;
   - DoD Directive 8500.1 Information Assurance;
   - AR 25-400-2, The Army Records Information Management System;
   - 10 USC 3013, Secretary of the Army.

   Consolidation would not result in additional forms of PII.

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.

   CAC number, Outlook GAL.

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.

   PBOs can produce reports that identify which equipment has been assigned to users. Users can access their own record that identifies the equipment assigned to them. The personally-identifiable information in these reports is only a user's name.

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.

   Users in DC and Afghanistan will use IDBS, and will access the same database, maintained by Army ITA. Consistent use of the system is enforced through policy (currently in draft form, in review by the AIG M&S).

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.

   The information stored in the IDBS is covered by the General Records Schedule. The General Records Schedules are issued by the Archivist of the United States to provide disposition authorization for records common to several or all of the agencies of the Federal Government. Specifically, the data is this system is covered by General Records Schedule 3, Procurement, Supply, and Grant Records, "Supply Management Files" and "Inventory Requisition Files."

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.

   Supply Management Files are to be destroyed when two years old, according to GRS 3, Disposition Authority NC1-64-77-5 item 5a. Inventory Requisition Files are to be destroyed 2 years from the date of the list, according to GRS 3, Disposition Authority NC1-64-77-5 item 10a. 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 the Corporation has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

   No. We have previously used CAC authentication in other applications.

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?

   Army ITA maintains the servers and network on which IDBS resides, and is responsible for data security. The Army identifies various DoD Components when generating PIAs for its own endeavors, including, but not limited to:

   - EO 9397 (SSN) as amended;
   - DoD Directive 8500.1 Information Assurance;
   - AR 25-400-2, The Army Records Information Management System;
   - 10 USC 3013, Secretary of the Army.

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

   SIGAR-08, Investigations 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?

   Yes. As a result of this process we are implementing an information audit function to ensure that records are kept of changes made to data in the system.

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

   Yes. See above.

Privacy Impact Assessment
Authorization Memorandum

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

	6/26/2012
System Manager	Date
	6/25/2012
Information Technology Security Manager	Date
	6/25/2012
Chief Privacy Officer	Date