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 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:	Investigations Directorate
System Name:	Investigative Case Management System
System Acronym:	ICMS
System Owner:	Special Inspector General for Afghanistan Reconstruction

A. Information and Privacy

ICMS is designed to fulfill the Special Inspector General for Afghanistan Reconstruction's (SIGAR) obligation to protect PII. ICMS meets 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:	Nicolaus R. Heun
Title:	Senior Investigative Analyst
Component:	Special Projects Office, Investigations Directorate, SIGAR
Address:	1550 Crystal Drive, Arlington, Va 22202

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

Name:	Nicolaus R. Heun
Title:	Senior Investigative Analyst
Component:	Special Projects Office, Investigations Directorate, SIGAR
Address:	1550 Crystal Drive, 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, 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 III
Title:	Director, Privacy, Records, And Disclosure
Component:	Office of General Counsel (OGC)
Address:	1550 Crystal Drive, Arlington, VA 22202

C. System Description

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

1. ICMS is a case management system used to retain, organize, and provide search capability of complaints, investigations, and relevant investigative information related to authorized investigations. PII retained in the system is compiled from relevant information obtained from other law enforcement agencies or offices of inspectors general; examination of investigative records; publically available sources, through interviews of complainants, witnesses, subjects, or other persons; and other authorized means.

2. ICMS stores and retrieves information by name, social security number, or unique identifier associated with an individual. ICMS is subject to a System of Record Notice (SORN) for investigations records.

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.

   ICMS is designed to retain descriptive information obtained in authorized investigations regarding investigative subjects, witnesses, or other relevant persons involved in an investigation. PII contained in ICMS may include the following descriptive information about a person: name, age, gender, address, telephone numbers, email addresses, social security number, date/place of birth, FBI number, passport number, military identification number, or other similar information.

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:

   ICMS is a federal law enforcement case management system designed to comply with the Privacy Act. Similar to other federal law enforcement systems, ICMS is not designed to allow an individual to "opt out" of the system.

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

   Information in ICMS is compiled from investigative information and reports provided by other law enforcement agencies and offices of inspectors general; regulatory information and reports obtained from state or federal regulatory or administrative agencies; publically available information relevant to authorized investigations, investigative examination of documents, records, or tangible things; information obtained in interviews of complainants, witnesses, subjects, or other persons; and other authorized means.

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.

   Federal agencies do not electronically transmit information for routine entry into ICMS. ICMS is updated on a case-by-case basis with information obtained from federal agencies including the Federal Bureau of Investigation, Department of Justice, Department of Defense components, Department of State components, and other federal agencies involved in investigating fraud, waste, or abuse concerning U.S. funds made available for the reconstruction of Afghanistan.

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.

   State and local agencies do not electronically transmit information for routine entry into ICMS. On a case-by-case basis, ICMS is updated with relevant information entered by investigators obtained from state or local agencies.

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.

   Other than the ICMS sources of information previously described, on a case-by-case basis, investigators may enter information into ICMS obtained from foreign law enforcement or regulatory agencies, including Government of Afghanistan law enforcement agencies and ministries assisting the U.S. in investigating fraud, waste, or abuse concerning U.S. funds made available for the reconstruction of Afghanistan.

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.

   ICMS is an internal electronic case management system with access is limited to SIGAR employees with a demonstrated need for access. ICMS data is not combined or united into another system, application, or process. The minimum sets of controls used are outlined in OMB Circular A-130, Appendix III, and the use of Role Based Access Controls (RBAC) is applied.

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.

   User access to ICMS is established by a "need-to-know" standard that requires approval by a SIGAR manager. User access rights are electronically obtained through DOD Common Access Card (CAC) authentication achieved through the user's issued CAC. Data stored on a user's CAC includes unique authentication data that ensures only the specified user obtains ICMS access through the CAC system. The user's CAC information is retained by ICMS and provides an audit trail. The criteria, procedures, controls, and responsibilities regarding access are documented to comply with Federal Information Security Management Act (FISMA) of 2002.

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

   ICMS access differs among user groups. Supervisors have greater access than investigators. General users have the ability to view all information within the system, except for grand jury material, confidential source information and internal investigations which are subject to specified access limitations. Some users are only able to view information pertinent to their particular region. Access is granted to the system based on their need to know and their job responsibilities within SIGAR.

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.

   Access is limited to investigative personnel. Technical controls at the application, server and network level exist to prevent unauthorized access and to limit data access based on a user's system rights and profile. Specifically, two levels of controls are in place to ensure that users cannot misuse data in ICMS. First, user access levels have been instituted to ensure that only authorized users may view material appropriate to their job responsibilities and that only users with a demonstrated need to know can access sensitive information. SIGAR application developers are upgrading the access audit function to produce reports on information that has been changed in the system. The upgraded audit function 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 ICMS administrators 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.

   ICMS shares information with the Army Global Address List and AKO for the purposes of CAC authentication. This limited access ensures that users are properly authenticated prior to gaining entry into ICMS.

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.

   Users with ICMS access are responsible for protecting personal information covered by the Privacy Act and are subject to administrative, civil, or criminal sanctions for misuse of ICMS information. ICMS users undergo privacy training that reinforces this responsibility.

   The public does not have access to the system. ICMS is only accessible on computers in which authenticated users have accessed the system via their CACs. Additionally, U.S. Army ITA maintains the servers and network on which ICMS resides and is responsible for ICMS 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.

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?

   ICMS information may be shared with other law enforcement agencies pursuant to a SORN or Privacy Act.

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 employees who have access to information in a Privacy Act system have responsibility for protecting personal information covered by the Privacy Act, often the information owner and system manager (identified in the Privacy Act system of records notice) share responsibilities. Annual refresher training is done at the agency level.

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

   The SIGAR Investigations Directorate conducts highly-sensitive criminal and civil investigations related to fraud, waste, and abuse in the reconstruction of Afghanistan that would be disrupted if PII is disclosed without authorization. For example, an unauthorized disclosure of PII may alert a subject of a criminal investigation to the government's interest and investigative direction thereby allowing the subject to hide assets, conceal evidence or otherwise thwart the government's investigation.

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?

    SIGAR contactor personnel signed confidentiality and non-disclosure agreements that cover ICMS information and SIGAR information and data.

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.

    Because this is an approved federal law enforcement system, the data owner will not be contacted.

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.

   Field interviews, public information and other law enforcement databases. Information contained in ICMS is often derived from sources of unknown credibility, as is often the case with law enforcement information, and ICMS, through the Investigations SORN, is exempt from some aspects of the Privacy Act.

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.

   Field interviews, public information and other law enforcement databases. Notwithstanding, some information contained in ICMS is often derived from sources of unknown credibility, as is often the case with law enforcement information, and ICMS, through the Investigations SORN, is exempt from some aspects of the Privacy Act. Data in the system itself will be reviewed by ICMS administrators to ensure that the system's data store is fully complete.

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. The Privacy Act at 5 U.S.C. 552a(e)(l) requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

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.

   Yes. Data is maintained in the database server for each individual.

ICMS may derive new data and create previously unavailable data about an individual(s) through aggregation of the information collected.

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.

   ICMS is an "internal" use only application. ICMS data is not consolidated, that is, combined or united into another system, application, or process. The minimum sets of controls used are outlined in OMB Circular A-130, Appendix III and the use of Role Based Access Controls (RBAC) is applied.

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.

   ICMS information is retrievable by name and, if available, social security number.

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.

   Reports can be generated summarizing information about individuals, and their role in criminal, civil and/or administrative investigations.
   These reports are available for use authorized SIGAR personnel with an identified "need to know" in the furtherance of official investigations.

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 can access ICMS from any web-enabled computer that has a CAC reader and appropriate security and CAC authentication software. However, the data itself resides on an ITA-maintained server. Users who access the system via the web do not have the rights to change system controls.

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 Investigative data in the ICMS until all investigative recommendations are closed. At that time, records will be transferred to Federal Records Center and maintained in accordance with SIGAR's Investigations 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.

   Investigative records will be retained, disposed, and transferred to the National Archives in accordance with the SIGAR Investigations 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, ICMS 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.

   Audit trails are maintained to record login attempts and the entry or update of system data. The SIGAR IT boundary Security C&A system security plan outlines the implementation of the technical controls associated with identification and authentication levels at the network level.

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.

   ICMS access is restricted to SIGAR employees with a "need-to-know". The system technology is similar to case management systems used by many federal law enforcement or offices of inspectors general.

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.

ICMS has the capability to identify users through IP addresses, web access logs and session information. The database maintains the time/date and identity of users entering or updating system information.

Audit trails are maintained to record logon attempts and the entry or update of system data. The SIGAR IT boundary Security C&A system security plan outlines the implementation of the technical controls associated with identification and authentication levels at the network level.

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

   Since ICMS data contains the SIGAR Investigations Directorate criminal investigations, and this formation has "Moderate" sensitivity, access is limited to staff with a legitimate need-to- know. SIGAR policy also makes staff accountability for protecting the integrity of the information very clear.

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

   SIGAR-08, Investigation 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?

   No.

Privacy Impact Assessment
Authorization Memorandum

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

Nicolaus N. Henn — 25 Jul 2012

System Manager — **Date**

Ward W. Hoag — 7/19/2012

Information Technology Security Manager — **Date**

Kate Gastner (acting) — 7/26/2012

Chief Privacy Officer — **Date**