Privacy Impact Assessment

OIG Audit & Investigations Management Systems (AIMS)

- Date: February 10, 2016
- Prepared by: USDA Office of Inspector General (OIG), Information Technology Division (ITD)

United States Department of Agriculture

Privacy Impact Assessment for the

OIG Audit & Investigations Management Systems (AIMS)

February 10, 2016

Contact Point
Kimberly Din
IT Specialist
Office of Inspector General
United States Department of Agriculture
202-720-8670

Reviewing Official
Craig Goscha
Chief Information Officer
Office of Inspector General
United States Department of Agriculture
816-926-7644

Abstract

The OIG Audit & Investigation Management Systems (AIMS) are owned and operated by the Office of Inspector General (OIG). AIMS is a collection of applications including ARGOS, TeamMate, ACL, and IA Professional (OCI) that are used in support of the primary business functions of OIG: Audits and Investigations. These applications provide the capability to store and retrieve information of individuals involved in various investigative cases, program related audits, and internal process management.

Overview

The Audit & Investigation Management Systems (AIMS) is owned and operated by the Office of Inspector General (OIG).

The purpose of the AIMS is to support OIG audits and investigations by providing the capability to store and retrieve information of individuals involved in various investigative cases, program related audits, and internal process management.

The information in the AIMS is typically obtained through USDA agencies and other law enforcement agencies as part of an effort to promote economy, efficiency, and effectiveness or that prevent and detect fraud and abuse in programs and operations, both within USDA and in non-Federal entities that receive USDA assistance.

The OIG ARGOS is an application system built specifically by OIG to store information for auditors about in-process and completed audits, for supervisors about employee training, security clearances, grade, salary, and time and attendance information, for FOIA staff for tracking FOIA requests and for investigators who are building cases for crimes committed against USDA policies. This system contains sensitive information regarding employees, security clearances, audits, investigative cases, etc.

ACL is a COTS data analysis software supporting OIG program, financial, and IT audits. The application provides a unique and powerful combination of built-in audit analysis commands, ad-hoc data access and a simple scripting language. It enabled OIG auditors to gain immediate visibility into transactional data critical to various audit projects.

TeamMate is a COTS suite of products that allow auditors to identify, schedule, document, report and track time and expenses on audits. The application streamlines and integrates every facet of the internal audit process, including: risk assessment, scheduling, planning, execution, review, report generation, trend analysis, committee reporting and storage.

IAPro is a COTS software application supporting the OIG Office of Compliance and Integrity (OCI) in the handling of employee complaints, administrative investigations, use-of-force reporting, and other types of incidents, while providing the means to analyze and identify areas of concern.

The Office of Inspector General was legislatively established in 1978 with the enactment of the Inspector General Act (Public Law 95-452). The act requires the Inspector General to independently and objectively perform audits and investigations of the Department's programs and operations.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

AIMS maintains information related to OIG investigations, audits, projects, and internal process management regarding personnel. The information may include the PII of USDA and non-USDA individuals (name, date of birth, address, personal identification number, criminal history, etc.).

1.2 What are the sources of the information in the system?

Information within AIMS originates from governmental employees, contractors, or other subjects of investigation or audits.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is being collected to perform a variety of tasks related to investigations, audit, administration, and FOIA.

1.4 How is the information collected?

The information is collected by trained investigators, auditors, administration staff, or provided by other USDA and non-USDA Agencies.

1.5 How will the information be checked for accuracy?

Information entered is reviewed by the employee and a manager.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Office of Inspector General was legislatively established in 1978 with the enactment of the Inspector General Act (Public Law 95-452). The act requires the Inspector General to independently and objectively perform audits and investigations of the Department's programs and operations.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The exposure/risk to privacy is low. The data collected is restricted to specific groups (Investigation, Audit, Management, FOIA, etc.) who must have governmental interest in the data. The potential for a data privacy incident can occur when PII is sent to other USDA and non-USDA entities for collaboration on a case. The risk is mitigated through the use of approved encryption techniques and data loss prevention measures.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information is being collected to perform a variety of tasks related to investigations (past and present criminal cases, hotline complaints, asset forfeiture, etc.), audits (USDA programs and operations), administration (employee data, inventory, time management, training, employee complaints and investigations, etc.), and FOIA (FOIA requests).

2.2 What types of tools are used to analyze data and what type of data may be produced?

Queries and reports are used to analyze data.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Commercial and publicly available data are used to advance criminal investigations in verifying the identity of a subject of an investigation or to provide relevant information on a company or a business owner to support audit findings.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access control is locked down to specified group members who have a governmental use for the data.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

All information contained will be retained in compliance with NARA Guidelines, which vary from five to ten years according to OIG Directive IG-2186 CH6.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Possible risks include unintentional disclosure during the retention period. Risks are mitigated through training on the sensitivity of information and the restrictions on disclosure. Information is retained in compliance with the records schedules and access is limited to employees with governmental needs.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information may be shared with internal USDA agencies on a need-to-know basis to further investigation or audit cases.

4.2 How is the information transmitted or disclosed?

The information may be transmitted through electronic mail or delivered via portable media such as a flash drive, optical media, or a hard drive. When necessary, data if encrypted per regulations using AES-256 encryption.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The greatest risk to the data occurs if portable media such as optical drives or flash drives are lost; however, this media is encrypted. Another possible risk is unintentional disclosure of sensitive information. This risk is mitigated through training our employees on the sensitivity of files and the restrictions on disclosure. Also, access to AIMS is limited to employees on a need-to-know basis.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information may be shared with other law enforcement agencies that are conducting the investigation jointly with the OIG and also shared with the United States Attorney's Office or the State/local prosecutor to further the investigative process towards an indictment.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, sharing of PII outside the Department is compatible with the original collection. This is covered by SORN USDA/OIG-5.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information is shared with other law enforcement agencies who are working the case jointly with OIG, and with the Department of Justice, United States Attorney's Office or State/local prosecutors. The data is encrypted per regulations using AES-256 encryption.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risks are minimal. The external agencies are law enforcement agencies that are covered by similar Privacy Act Systems of Records and are being provided the information on a need-to-know basis to assist in furthering the investigative process.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice to all individuals is provided in the SORN published in the Federal Register which describes what information is collected, its purpose, how it will be used, where it will be stored, how it is secured, and where an individual may place a request.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The information contained in AIMS is used to support OIG investigations, audit, and for personnel matters. This information is integral to the OIG purpose and function as provided in the SORN. This information is used for official OIG operations and is not accessible to non-OIG personnel or to unauthorized OIG personnel without a valid work requirement.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals can only request access to their records under the Freedom of Information Act (FOIA).

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals desiring to contest or amend information maintained in the system should direct their request to the OIG Assistant Inspector General for Policy Development and Resources Management and should state clearly what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

7.3 How are individuals notified of the procedures for correcting their information?

Notice is provided in the corresponding SORN, USDA/OIG-5: Federal Register Volume 73, No. 144/Friday, July 25, 2008.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is provided as stated above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Redress measures are provided to individuals. When an individual makes a FOIA request and if they identify inaccurate information and request that it be corrected, OIG will respond to the correction request.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Managers are responsible for requesting individuals' access to specific modules where information is housed. IT Specialists are responsible for assigning the necessary permissions. Permissions are documented. OIG personnel that access the system use their ID and password to access records that they have been approved to view and/or update.

8.2 Will Department contractors have access to the system?

OIG contractors that have a business need to have access to the system are assigned a user account and granted the necessary permissions.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All privacy training pertaining to this system is apropos to the training required to access the OIG network.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

User activity on AIMS is logged to ensure the scope of their activity does not exceed their authority.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Possible privacy risks include unauthorized access. Security controls such as limited access and audit trails mitigate this risk. For remote access, a two-factor authentication system is required to access the OIG network, followed by the use of additional username and password to access specific data.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

This is a system that is currently in its operation and maintenance phase.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not Applicable

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not Applicable

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable

10.10 Does the system use web measurement and customization technology?

Not Applicable

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

Not Applicable

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable

Responsible Officials

Craig Goscha, Chief Information Officer, Office of Inspector General, United States Department of Agriculture

Kimberly Din, Acting Information Systems Security Program Manager, Office of Inspector General, United States Department of Agriculture

Approval Signatures

Craig M Goscha

DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=CRAIG GOSCHA, 0.9.2342.19200300.100.1.1=12001000698835
Date: 2016.02.10 19:18:07 -06'00'

_____

Craig Goscha
Chief Information Officer
Office of Inspector General
United States Department of Agriculture

KIMBERLY DIN

Digitally signed by KIMBERLY DIN
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=KIMBERLY DIN, 0.9.2342.19200300.100.1.1=12001000211619
Date: 2016.02.10 08:43:10 -05'00'

_____

Kimberly Din
Information Systems Security Program Manager (Acting)
Office of Inspector General
United States Department of Agriculture