

United States Department of Agriculture (USDA)
1400 Independence Avenue, SW
Washington, DC 20250

OFFICE OF THE INSPECTOR GENERAL (OIG)
ARGOS
MAJOR APPLICATION (MA)



PRIVACY IMPACT ASSESSMENT (PIA)

December 2006

Prepared by:

OIG

Information Technology Division

Distribution limited to U.S. Government agencies and USDA contractors only.
Requests for this document must be referred to the Office of the Inspector General.

FOR OFFICIAL USE ONLY

| Agency/Reviewer | PG # | PARA # | LINE # | COMMENTS |
|-----------------|---------|-----------|-----------|----------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

A. GENERAL SYSTEM/APPLICATION INFORMATION

1. System Owner:

| Name | Title | Phone No. | Office |
|------------|--------------|----------------|---------|
| Rod DeSmet | CIO, AIG OIR | (202) 720-5168 | OIG/OIR |

2. Other individuals completing this form:

| Name | Title | Phone No. | Office |
|-------------------|----------------------|----------------|-----------------|
| Rosemary Gilhooly | IT Division Director | (202) 720-3089 | OIG/IT Division |
| Mahmood Morid | ISSPM | (202) 720-7423 | OIG/IT Division |
| | | | |

3. System/Application Name: System - USDA Office of Inspector General's ARGOS SYSTEM.

Briefly describe the purpose of this system:

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 policy. ARGOS is an existing system with many modules, the first of which went into production in October 2001. This system contains sensitive information regarding employees, case files, security clearances, audits, etc. The system consists of four servers; two in Washington, DC and two in Kansas City, MO. The two main servers are UNIX and execute an Oracle database for ARGOS, version 8.1.7. The remaining servers are a Forms server and a Web server both running Microsoft Server 2000. All ARGOS data resides on the Unix servers. The Forms servers provide access to the information. There are approximately 625 personnel in OIG, most of whom are remote users, who have access to ARGOS based on their specific job responsibilities.

4. Describe what agency function/mission does it support?

The mission of the Office of the Inspector General (OIG) is to promote effectiveness and integrity in the delivery of USDA agricultural programs.

B. SYSTEM DATA INFORMATION

1.0 Generally describe the information to be used in the system:

Administrative Data related to Employees; Audit Data related to Audits performed by the Agency; Investigations Data related to Investigations made by the Agency; and Inspections Data related to Inspections conducted by the Agency.

1.1 What information is to be collected?

Information collected in ARGOS depends on the module. ARGOS data can be classified into four categories; Investigations, Audit, Inspections and Administration. There are multiple modules within the four categories. The individual breakdown of data attributes follows:

1.2 Investigations.

- a. Asset Forfeiture Information including owner's information.
- b. Complainant Information – Individuals who have not requested anonymity or confidentiality regarding identity, who allege wrongdoing.
- c. Confidential Informant Information.
- d. Investigative Operatives.
- e. Principal Information – Individuals; not named subjects, who may be responsible for wrongdoing.
- f. Others – Individuals closely connected with a matter of investigative interest.
- g. Supoena System for generating and tracking Subpoenas.
- h. Subject Information – Individuals against whom allegations of wrongdoing have been made.
- i. Undercover OIG Special Agent and other Law Enforcement Information.

1.3 Audit.

No personal information is kept in the Audit Module about persons who are not federal government employees or contractors.

1.4 Administration.

- a. EEO Information regarding complaints of discrimination.
- b. Employee Security Clearance Information.
- c. Employee Tracking Information including employee personal information, emergency contact information, emergency room assignments, onsite duty stations, official duty station moves, property incidents and claims, awards, and training.
- d. Technical Equipment Inventory including IP Address assignments, Laptop serial numbers, and other IT equipment assigned to employees.
- e. Time Management System for recording employee hours worked with daily hourly totals by pay period including NFC salary and leave data downloaded from NFC.

1.5 Inspections.

The Inspections Tracking module is currently under development. It currently does not contain any data. Access to the module will be limited to Inspections staff. The module will contain tracking data for managing Inspections and will be referenced by Inspection Case Number. This module will not contain any PIA data.

1.6 FOIA.

The FOIA module tracks the status of FOIA/PA and Appeals requests, including any Audit reports, Investigations reports, Inspections reports or IG Manual sections involved in the FOIA request.

2.0 Why is the information being collected?

This information is being collected to perform a variety of tasks most of which are routine. These uses are identified in existing OIG System of Records submissions available in the Federal Register. Below is an excerpt from the Federal Register that describes the routine uses.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

- a. A record from the system of records which indicates either by itself or in combination with other information, a violation or potential violation of a contract or of law, whether civil, criminal, or regulatory, or which otherwise reflects on the qualifications or fitness of a licensed (or seeking to be licensed) individual, may be disclosed to a federal, state, local, foreign, or self-regulatory agency (including but not limited to organizations such as professional associations or licensing boards), or to another public authority that investigates, prosecutes or assists in such investigation, prosecution, enforcement, implementation, or issuance of the statute, rule, regulation, order, or license.
- b. A record from the system of records may be disclosed to a federal, state, local, or foreign agency, as well as other public authority, including consumer reporting agency, or professional organization maintaining civil, criminal, or other relevant enforcement or other pertinent records, such as current licenses, in order to obtain information relevant to

an OIG decision concerning employee retention or other personnel action, issuance of a security clearance, letting of a contract or other procurement action, issuance of a benefit, establishment of a claim, collection of a delinquent debt, or initiation of an administrative, civil, or criminal action.

- c. A record from the system of records may be disclosed to a federal, state, local, foreign, or self-regulatory agency (including but not limited to organizations such as professional associations or licensing boards), or to another public authority, to the extent the information is relevant and necessary to the requestor's hiring or retention of an individual or any other personnel action, issuance or revocation of a security clearance, license, grant, or other benefit, establishment of a claim, letting of a contract, reporting of an investigation of an individual, for purposes of a suspension or debarment action, or the initiation of administrative, civil, or criminal action.
- d. A record from the system of records may be disclosed to any source, private or public, in order to secure source information relevant to a legitimate OIG investigation, audit, inspection or other inquiry.
- e. A record from the system of records may be disclosed to the Department of Justice in the course of litigation, when the use of such records is deemed relevant and necessary. A record may be disclosed in a proceeding before a court, an adjudicative body, an administrative tribunal, or in the course of civil discovery, litigation, or settlement negotiations, when a part to a legal action, an entity or and an individual having an interest in the litigation includes any of the following:
 - 1. The OIG or any component thereof.
 - 2. Any employee of the OIG in his or her official capacity.
 - 3. Any employee of the OIG in his or her individual capacity where the Department of Justice has agreed to represent the employee.
 - 4. The United States, where the OIG determines that litigation is likely to affect USDA or any of its components.
- f. A record from the system of records may be disclosed to a member of Congress from the record of an individual. This may be done in response to a request made by that individual. In such cases however, the member's right to a record is no greater than that of the individual.
- g. A record from the system of records may be disclosed to the Department of Justice for the purpose of obtaining its advice on an OIG audit, investigation, inspection or other inquiry, including Freedom of Information or Privacy Act matters.
- h. A record from the system of records may be disclosed to the Office of Management and Budget for the purpose of obtaining advice regarding OIG obligations under the Privacy Act or during the review of private relief legislation.

- i. A record from the system of records may be disclosed to a private firm with which OIG contemplates it will contract or with which it has contracted for the purpose of performing any functions or analyses that facilitate or are relevant to an OIG investigation, audit, inspection, or other inquiry. Such contractor or private firm will be required to maintain Privacy Act safeguards with respect to such information.
- j. A record from the system of records may be disclosed in response to a subpoena issued by a federal agency that has the power to subpoena records of other federal agencies if the OIG determines that:
 - 1. The records are both relevant and necessary to the proceeding.
 - 2. Such release is compatible with the purpose for which the records were collected.
- k. A record from the system of records may be disclosed to a grand jury agent pursuant either to a federal or state grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury, provided that the grand jury channels its request through the cognizant United States Attorney, that the United States Attorney has been delegated the authority to make such requests by the Attorney General, and that the United States Attorney actually signs the letter specifying both the information sought and the law enforcement purpose. In the case of a state grand jury subpoena, the state equivalent of the United States Attorney and Attorney General shall be substituted.
- l. A record from the system of records may be disclosed, as a routine use, to a federal, state, local, or foreign agency, or other public authority, for use in computer matching programs. These programs are used to prevent and detect fraud and abuse in benefit programs administered by any agency. They also support civil and criminal law enforcement activities of any agency and its components. The programs are further used to collect debts and overpayments owed to any agency and its components.
- m. Relevant information from a system of records may be disclosed to the news media and general public where there exists a legitimate public interest, *e.g.*, to assist in the location of fugitives, to provide notification of arrests, or where necessary for protection from imminent threat of life or property.
- n. A record may be disclosed to any official charged with the responsibility to conduct qualitative assessment reviews or peer reviews of internal safeguards and management procedures employed in investigative operations. This disclosure category includes members of the President's Council on Integrity and Efficiency and officials and administrative staff within their investigative chain of command, as well as authorized officials of the Department of Justice and the Federal Bureau of Investigation.

- o. In the event that these records respond to an audit, investigation or review, which is conducted pursuant to [*21390] an authorizing law, rule or regulation, and in particular those conducted at the request of the President's Council on Integrity and Efficiency ("PCIE") pursuant to Executive Order 12993, the records may be disclosed to the PCIE and other Federal agencies, as necessary.

3.0 What is the intended use of the information?

There are 15 routine uses for this information. (See answer to #2)

4.0 With whom will the information be shared?

Information is shared with the Chief Financial Officer and National Finance Center.

A weekly report is sent to the CFO's office detailing current audit assignments, the auditor recommendations, the status of the recommendations and the monetary considerations.

The Time Management module produces a report which is used by Timekeepers to enter employee time and attendance data into NFC.

This information is distributed in the form of reports in PDF format or Excel spreadsheets. Only OIG employees have access to ARGOS. External systems are not permitted to access any module of ARGOS.

5.0 What Federal Agencies are providing data for use in the system?

Each pay period the National Finance Center provides OIG employee information such as salary, pay-plan and grade which is loaded into the database.

6.0 From what other third party sources will data be collected?

None

7.0 What information will be collected from the customer/ employee?

No data is directly collected from customers. OIG Employees enter time and attendance data on a weekly basis. OIG employee emergency contact information is also collected and periodically verified and updated.

8.0 How will data be collected from sources other than USDA records and the customer?

N/A

9.0 How will data be checked for completeness?

Quality control programs are run to ensure the data is entered correctly.

C. ACCESS TO THE DATA

1.0 Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Access to records in the system is limited to authorized personnel whose official duties require such access including Auditors, Investigators, Supervisors, DBA, System Developers and other Employees of OIG. Employees only have access to the modules they require to perform their job.

2.0 How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?

User access to information is limited by the permissions assigned by their supervisor. Criteria, procedures, controls, and responsibilities regarding access are currently not documented.

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

Access to records in the system is limited to authorized personnel whose official duties require such access, and on the principle of least privilege. Data is protected through user identification, passwords, database permissions and software controls. Such security measures establish different access levels for different types of users. As with most systems, Data Base Administrators (DBA) have access to all information stored in the Data Base Management System (DBMS). Additionally, certain modules within ARGOS implement encryption techniques within the database to further enhance the confidentiality and integrity of the information.

Physical security mechanisms are also in place to protect the information. ARGOS database servers are housed in secure computer facilities in Washington, DC and Kansas City, MO. These facilities have access control, fire suppression, air conditioning and uninterrupted power source (UPS). Data backups are performed according to established procedures.

4.0 What controls are or will be in place to prevent the misuse (i.e. unauthorized browsing, unauthorized use) of data by those having access?

Database Roles, Privileges and Application Roles are in place for each function performed in the system and audits of these controls are tracked by ARGOS. All access to reports containing PIA data is logged and the Privacy Officer reviews this log monthly.

5.0 Do other systems share data or have access to data in this system? If yes, explain.

Information is shared with the Chief Financial Officer and National Finance Center.

A weekly report is sent to the CFO's office detailing current audit assignments, the auditor recommendations, the status of the recommendations and the monetary considerations.

The Time Management module produces a report which is used by Timekeepers to enter employee time and attendance data into NFC.

This shared information is distributed in the form of reports in PDF format or Excel spreadsheets.

Only OIG employees have access to ARGOS. External systems are not permitted to access any module of ARGOS.

Each pay period the National Finance Center provides OIG employee information such as salary, pay-plan and grade which is loaded into the database.

6.0 Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface?

The privacy rights are protected by OIG Management and implemented by the ARGOS System Administrators (SA) and Database Administrators (DBA).

7.0 Will other agencies share data or have access to data in this system (International, Federal, State, Local, and Other)? If yes, explain.

See answer to 5.

8.0 How will the data be used by the agency?

The Audit, Inspections and Investigations Systems are used by Auditors, Investigators, Inspectors and their Managers to track, record, and monitor the Status of Audits, Inspections and Investigations. The system provides most of the data that is used to prepare the SARC (Semi Annual Report to Congress) Reports to Congress detailing the work of the Agency. Administrative modules are used by the Agency's Administrative Staff and OIG Management to manage the Agency's (approximately) 610 Employees.

9.0 Who is responsible for assuring proper use of the data?

OIG Management

D. ATTRIBUTES OF THE DATA

1.0 Is the use of the data both relevant and necessary for the purpose for which the system is being designed?

Yes.

2.0 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

3.0 Will the new data be placed in the individual's record (customer or employee)?

N/A

4.0 Can the system make determinations about customers or employees that would not be possible without the new data?

N/A

5.0 How will the new data be verified for relevance and accuracy?

N/A

6.0 If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A

7.0 If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

N/A

8.0 How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Modules that allow for searching by employee names are linked to a system generated employee id field to link records to employee names in the Master Table. Audit, Inspections and Investigations searches use Case Numbers and Assignment Numbers when querying the data. The Employee Tracking Module is the only module that allows a search on social security number. Access to this module is tightly controlled. PIA data has been removed from all reports except those for which it is absolutely necessary.

9.0 What are the potential effects on the due process rights of customers?

There is no new technology impact that will affect due process rights of customers or employees

10.0 How are the effects to be mitigated?

N/A

E MAINTENACE OF ADMINISTRATIVE CONTROLS

1.0 Explain how the system and its use will ensure equitable treatment of customers and employees?

N/A

2.0 If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

System replication mirrors transactions from one site to another across a dedicated circuit. Programming changes are also replicated.

3.0 Explain any possibility of disparate treatment of individuals or groups.

N/A

4.0 What are the retention periods of data in this system?

Information retention is in accordance with the Agencies' records maintenance and disposition schedule.

5.0 What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

Before destroying official files, determine the appropriate method of destruction based on the sensitivity of the material in the files. Wipe data such as correspondence logs, employee performance records, investigative files, and any other material which may contain names of individuals, allegations, or other sensitive information.

The procedures are documented in OIG Directive IG-2186.

6.0 While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Data Entry and Supervisory Personnel run reports on this data. ARGOS maintains point in time information for all data changes and for auditing, inspection and investigations purposes.

7.0 Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller ID)?

No

8.0 How does the use of this technology affect customer/employee privacy?

N/A

9.0 Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system provides the capability to identify and locate individuals. It monitors access to reports containing identifying data on individuals.

10.0 Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No.

11.0 What controls will be used to prevent unauthorized monitoring?

Access is limited by controlled assignment of user ID, password, and responsibility. Each responsibility comes with a predetermined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user.

12.0 Under which Systems of Record (SOR) Notice does the system operate? Provide number and name.

62 Fed. Reg. 61262

13.0 What opportunities will individuals have, if any, to decline to provide information or to consent to particular uses of the information?

Contesting record procedures: An individual may contest information in this system which pertains to him/her by submitting a written request to the Assistant Inspector General for Management, Office of Inspector General, United States Department of Agriculture, Washington, DC 20250-2310.

To request access to information in this system write to the FOIA Office, Office of Inspector General, United States Department of Agriculture, Washington, DC 20250-2309.

The following is an excerpt from the OIG System of Record Notices (SORN) in the Federal Register. Some information in ARGOS modules is exempt from provisions of the Privacy Act per the statute listed in the next two paragraphs.

Systems exempted from certain provisions of the act: Pursuant to 5 U.S.C. 552a(j)(2), this system of records has been exempted from all provisions of the Privacy Act of 1974, 5 U.S.C. 552a, as amended, except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i).

Pursuant to 5 U.S.C. 552a(k)(2) and (k)(5), this system has been exempted from the following provisions of the Privacy Act of 1974, 5 U.S.C. 552a: subsections (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

14.0 Is the system of records being created under section 552a of title 5, United States Code?

Yes.

Note: This PIA must be submitted separately to PIA@omb.eop.gov.

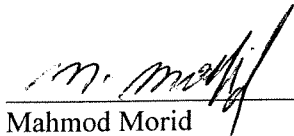
Analysis: As a result of this PIA, OIG will not change ARGOS or its information collection process.

Certifications:

Mahmood Morid
Office of the Inspector General,
USDA
Phone: (202) 720-7423
E-mail: MMORID@oig.usda.gov
Signature:

Wilbur Crawley
Office of the Chief Information
Officer, USDA
Phone: (301) 504-4154
E-mail:
wilbur.crawley@usda.gov
Signature:

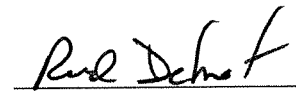
Rod DeSmet
Office of the Inspector General,
USDA
Phone: (202) 720-3089
E-mail: Rod.DeSmet@oig.usda.gov
Signature:

 12/19/06

Mahmood Morid Date

IT Security Specialist

Privacy Policy Analyst Date

 12-19-06

Rod DeSmet Date
Chief Information Officer

