Privacy Impact Assessment

Integrated Acquisition System (IAS)

Revision: 1.0

Office of Procurement and Property Management (OPPM)
Procurement Services Division (PSD)

Date: June 25, 2010

Prepared By:
SeNet International

Document Information

Owner Details	
Name	Nicole Gray
Contact Number	202-720-8612
E-mail Address	Nicole.Gray@DA.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	02/24/2010	SeNet International	Initial DRAFT

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**

Table of Contents

1 SYSTEM INFORMATION

System Information	
Agency:	Office of Procurement and Property Management (OPPM) Procurement Services Division (PSD)
System Name:	Integrated Acquisition System (IAS)
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	IAS is a suite of commercial off the shelf software (COTS) applications with a custom interface that is used for administrative acquisition management through the United States Department of Agriculture (USDA). The overall purpose of IAS is to solve several administrative business issues and to meet federal financial and acquisition requirements. IAS ensures that all procurement and financial data generated by any program or agency within USDA is contained in a single source with a standardized format for use in any procurement or acquisition processes. IAS is a major application in the operational phase of the system development life cycle. To achieve this mission, IAS interfaces with the core USDA financial system called the Foundational Financial Information System (FFIS).
Who owns this system? (Name, agency, contact information)	Michael McFarland PSD – Information System Owner 501 School St – 3rd Floor Washington, DC 20024 (202) 401-1023 michael.mcfrarland@da.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Nicole Gray PSD – Information System Security Program Manager 501 School St – 3rd Floor Washington, DC 20024 (202) 557-1754 Nicole.gray@da.usda.gov
Who completed this document? (Name, agency, contact information)	Nicole Gray PSD – Information System Security Program Manager 501 School St – 3rd Floor Washington, DC 20024 (202) 557-1754 Nicole.gray@da.usda.gov

2 DATA INFORMATION

This chapter includes information on data collection, data use, data retention, data sharing, data access, and customer protection.

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	The data contained in the IAS system can be divided into two categories: seed data, which is that data needed to support all functions of the system, and transaction data, which is that data created by users in using the system. The seed data is divided into four primary categories: user data, vendor information, account code information, and other referential data needed to support the functions of the system. Other referential data refers to enterprise payment terms, office addresses, product service codes, and units of measure. Transactional data will be transactions created by the user and will consist of documents and transactions. The documents created are requisitions and awards. The transactions created are requisition approvals, award approvals, receipt entries, and invoice entries and associated approvals. *Customer related data includes:* *First Name, Middle Name, Last Name, Phone Number, Fax Number, Street Address, City, State, Zip Code, Country, E-Mail Address, Tax Identification Number and/or Social Security Number* *Employee related data includes:* *Name, Last Name, Office Phone Number, Office E-Mail Address*
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	□ Yes ☒ No – If No, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes □ No

No.	Question	Response
4	Sources of the data in the system.	Sources of USDA information for IAS originates from the USDA agencies acquisition and budget execution transactions/documents, such as contracts, statements of work, requisitions, etc. entered into the IAS system. Seed data for vendors and account codes will be drawn from the Foundation Financial Information System (FFIS) once the interface between IAS and FFIS goes into production. Sources = FFIS, USDA employees, vendor and contractors
4.1	What data is being collected from the customer?	Each agency implemented into IAS shares a common database that is logically separated through the use of data and user profiles. IAS agencies configurations are developed and implemented during agency configuration workshops. IAS agencies share a common database that contains enterprise level data such as vendor information, common clauses, etc., and also contains agency specific information and data. All IAS data, enterprise and/or agency level is physically located in a common Oracle database system. Customer: First Name, Middle Name, Last Name, Phone Number, Fax Number, Street Address, City, State, Zip Code, Country, E-Mail Address; Employee: First Name, Middle Name, Last Name, Office Phone Number, Office Fax Number, Office Street Address, City, State, Zip Code, Country, Office E-Mail Address
4.2	What USDA agencies are providing data for use in the system?	There are currently 4 USDA agencies that are implemented using IAS. Food and Nutrition Service (FNS), and Rural Development have completed their agencies' rollout to implement IAS. . The Natural Resource Conversation Service (NCRS) and the Food Safety Inspection Services (FSIS) completed initial rollouts by the end of FY'03 with the possibility of some addition of more users in the future. The Forest Service has implemented the solution to a limited user base. During FY2004, the user base will expand to include additional Forest Service users and a selected group of users from the Associate Chief Financial Officer – Financial Operations (ACFO-FO), Controller Operations Division (COD) Administrative Payments Branch (APB) will be added to IAS for purposes of invoice entry and payment scheduling.

No.	Question	Response
4.3	What state and local agencies are providing data for use in the system?	There are no state or local agencies that are providing data for use with IAS
4.4	From what other third party sources is data being collected?	N/A
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or non-USDA sources.	☒ Yes ☐ No – If No, go to question 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Using internal business processes and rules and input / output validation is done through E-Authentication process.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	GSA will provide FAC updates to the FAR as well as NAICS and Product Service Codes to the vendor. Agency team members responsible for reviewing and utilizing the provided updates will verify the collected data using multiple mechanisms such as agency reports as well as direct queries to the IAS.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	There is a series of checks and edits that IAS performs to ensure that all the data elements are in place in any incoming data. It also reconciles the number of records that were staged to process through with the number actually processed to ensure there is a match. The IAS – FFIS interface also supports a consistency check process that will identify records out of balance so that resolution can be undertaken to ensure both completeness and consistency of data common to both systems. Business rules and input / checks will be used to ensure that the expected inputs and outputs are consistently provided.

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	To obtain access to the IAS, Employees provide employee name, employee work location, employee work phone number, employee work electronic mail (e-mail) address, and agency requisition/contracts approver name(s) via IAS user data templates, through the IAS Help Desk, and in some cases may be updated through the user preferences in the system.

No.	Question	Response
7	Will the data be used for any other purpose?	□ Yes ☒ No – If No, go to question 8.
7.1	What are the other purposes?	
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes The use of the data in IAS is necessary to ensure reliable and accurate USDA-wide, procurement-related financial information and data. It is also important to support acquisition management activities of the agencies within the USDA. Information collected on individuals and business is also necessary for the prompt payment of agency obligations. □ No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists)?	□ Yes ☒ No – If No, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	□ Yes ☒ No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	□ Yes ☒ No The system does not provide the ability to make any determinations about employees that is not otherwise possible. Through management reporting tools present in IAS, the solution allows users to see how many solicitations were sent to given vendors and how many responses were received. The system also allows users to see how many awards were given to vendors. Managers may also use the reporting capability in IAS to assign award activities based on buyer workloads. All of this aforementioned functionality is based on a user's agency.
9.3	How will the new data be verified for relevance and accuracy?	N/A
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	To obtain access to the IAS, Employees provide employee name, employee work location, employee work phone number, employee work electronic mail (e-mail) address, and agency requisition/contracts approver name(s) via IAS user data templates, through the IAS Help Desk, and in some cases may be updated through the user preferences in the system.

No.	Question	Response
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If No, go to question 12.
11.1	What are the other uses?	
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If No, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	There is restricted access on the systems and monitoring of any attempts at unauthorized access. Access to all IAS functions and data is managed through the application of standard security groups and user profiles.
13	Are processes being consolidated?	☒ Yes ☐ No – If No, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	There is a set of internal controls and reviews conducted to prevent unauthorized access. Protection of data is a multi-layered approach. There is restricted access based on the user ID within the system, monitoring by Security Administrators and Management for unauthorized access attempts, and security audits are conducted on the system.

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☐ No – If No, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Data in the IAS will accumulate over time and will include historical data. Files/data will be kept for a minimum of six years to comply with Federal Acquisition Regulations regarding records retention for procurement actions.
14.2	What are the procedures for purging the data at the end of the retention period?	No files or data have been eliminated because the system is newly implemented. Data archiving processes are in the concept phase and will be developed and implemented in accordance with Federal regulations and requirements.

No.	Question	Response
14.3	Where are these procedures documented?	No files or data have been eliminated because the system is newly implemented. Data archiving processes are in the concept phase and will be developed and implemented in accordance with Federal regulations and requirements.
15	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?	Audits require that data be retained. The data is accurate because the checks the system does will show if the system is out of balance. As noted above, data from FFIS will be updated in real time as well as periodically refreshed, and checked for consistency between IAS and FFIS.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☒ Yes ☐ No – If No, go to question 18.
17.1	How will the data be used by the other agency?	FPDS Data from IAS will be shared with GSA. This is currently done by extracting the FPDS file from IAS and uploading it to GSA's FPDS Reporting System.
17.2	Who is responsible for assuring the other agency properly uses the data?	The agencies, the OPPM, users, managers, contractors, and Functional and Security Administrators all have the responsibility to assure the proper use of the data.
18	Is the data transmitted to another agency or an independent site?	☒ Yes ☐ No – If No, go to question 19.
18.1	Is there an appropriate agreement in place to document the interconnection and ensure the Personally Identifiable Information (PII) and/or Privacy Act data is appropriately protected?	Yes – IAS has interconnection agreements with FFIS, FMMI and EMD. No – The interconnection agreement between PSD and FPDS-NG is currently under development..
19	Is the system operated in more than one site?	☒ Yes ☐ No – If No, go to question 20.

No.	Question	Response
19.1	How will consistent use of the system and data be maintained in all sites?	The IAS systems are operated at one site, but they will be accessed across the United States and some foreign sites. All IAS data accessed will be located at the IAS host site – The National Finance Center (NFC) in New Orleans, LA. The IAS disaster recovery site is located at the NITC George Washington Carver Center (GWCC) located in Beltsville, MD. IAS security criteria, rules, procedures and documentation are used by all users regardless of location to ensure universal compliance with security policy.

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	IAS Users will have access to the data in the system based on job function and the need-to-know the information. They will be located throughout the USDA agencies, at the USDA's National Information Technology Center, and the National Finance Center. Users are allowed to enter documents and are given the average override level in order to override errors that are less severe and that may occur more often. Security profiles are set up for users to ensure that internal controls and separation of duties are maintained. The only IAS users who are indicated as being approved for access to the PVND table are individual contracting officers (to be selected at the user agencies). This will represent a small portion of the overall total user population of IAS. PVND transactions are transmitted through the interface between IAS and FFIS. This means that data is sent with specific user identifications through a secure VPN line to FFIS. Once the data is loaded into FFIS, then the FFIS access and security protocols obtain. This applies in reverse to the transmission of a new vendor record from FFIS to IAS. Sensitive information is restricted from users if there is no valid job-related need for the information to perform the duties of their position. If job duties include providing reports, then users will have access to the required data to run queries against the data. Managers within the agencies will have access that is based on their job function and the need-to- know the information. They have the ability to approve documents that require approvals, but they are not able to approve documents

No.	Question	Response
		they enter themselves. They have the highest override authority in case of severe errors that need to be overridden. System Administrators, which are the Functional Administrators and the Security Administrator in the IAS, have access to the data to perform their job functions. Functional Administrators set parameters for the nightly cycle, check and make changes as necessary to the reference tables in the system to ensure data integrity, and review system reports to ensure the system is in balance. Security Administrators manage the security tables within the IAS. It is their job function to manage the user's authority to update tables within the IAS, ensure the settings on the security tables reflect internal controls and monitor the system logs to check for unauthorized access, overrides and approvals. The IAS Operations team has access to maintain the system databases and files for the IAS. This requires that high-level access be given based on the job function. Their authority includes changing programs, modifying table structure, managing the servers, and processing files in the IAS. The systems developers also have appropriate access to view the data to ensure it is correct. Access is only granted after appropriate background investigations have been completed for this sensitive position. These users are located at the Office of the Chief Information Officer George Washington Carver Center (GWCC) and the Office of the Chief Information Officer National Information Technology Center. The USDA also has contractors that have access to the IAS system. They have access that is limited to the functions set forth in the contract. The contractors perform various roles based on their function including applications configuration, application support, and operational support. Contractors undergo background checks before they are allowed to access any data within the system. Access to all systems is protected by authentication, authorization, encryption of passwords, and password aging. Security background investigations are required of all users and contractors. All users, including contractors, have had security briefings about system security rules and must sign a document confirming that they understand the rules. IAS access = USDA users, system

No.	Question	Response
		administrators, security administrators, system developers and system operations and management staff.
21	How will user access to the data be determined?	Once a user has completed the background investigation required for Federal employment or being a contractor to the Federal Government, then access is granted based on job function and the need-to-know principle. A user signs a document (AD 1143) acknowledging that they have read and understand the system's security rules before access is granted. This document is kept on file with an original signature. The Security Administrator assigns a profile to the user based on their job functions after the request is signed. These profiles have been set up to provide access to only the data and application functions necessary to perform their job functions. Access to all IAS functions and data is managed through the application of standard security groups and user profiles. Only authorized users will be allowed to access the IAS system. E-Authentication will be required to access the system and users will complete the process to receive access credentials.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No
22	How will user access to the data be restricted?	The Security Administrator will monitor the systems security audit trail logs and reports to management, any types of unauthorized access attempts, overrides or approvals. The principle of least privilege is employed on this system. User's access will be restricted based on user role. Only an Administrator would have access to all data. An extremely restricted number of administrators will be designated.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No

2.6 Customer Protection

No.	Question	Response

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	All users, agencies and the Office of Procurement and Property Management (OPPM) have this responsibility. The IAS PMO has implemented numerous controls within the IAS solution including encryption and restricted access to data and functionality to protect employee's privacy data. These controls will be extended to the IAS-FFIS interface when it is implemented. Further, IAS users who trigger transactions in FFIS will have access as identified users to FFIS, and those user identifications will fall under the FFIS security profiles.
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	The IAS PMO has implemented numerous controls within the IAS solution including encryption and restricted access to data and functionality to protect employee's privacy data.
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If Yes, go to question 27. ☐ No
26.1	If No, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	Consider the following: ▪ Consolidation and linkage of files and systems ▪ Derivation of data ▪ Accelerated information processing and decision making ▪ Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If No, go to question 28.
27.1	Explain how this will be mitigated.	Security policy, procedures, oversight and reviews are implemented to mitigate the effects in all these systems. The applicable controls implemented within the IAS are in compliance with JFMIP, USDA OCIO Cyber Security guidance, NIST and FISCAM requirements.
28	How will the system and its use ensure equitable treatment of customers?	N/A
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If No, go to question 30
29.1	Explain.	

3 SYSTEM OF RECORD

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes □ No – If No, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	Yes, acquisition data can be retrieved by personal identifier, user name, for activity reporting data. The information contained in the IAS can retrieve data on this system by running reports and online viewing. Access to this data is restricted by role, whether data is agency or enterprise specific, and a need-to-know basis.
30.2	Under which System of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov).	The IAS and FFIS interface is expected to be implemented during Q2 of FY2004 and at that time will be subjected to the applicable SOR notices for FFIS and IAS. These SORs will be identified at that time.
30.3	If the system is being modified, will the SOR require amendment or revision?	☒ Yes □ No

4 TECHNOLOGY

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	☐ Yes ☒ No – If No, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	

5 COMPLETION INSTRUCTIONS

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

____
(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

____ ______________
System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

____ ______________
Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

____ ______________
Agency OCIO

Date