Privacy Impact Assessment

Integrated Acquisition System (IAS) Major Application (MA)

- Version: 2.1
- February 2020
- OCP PSD IAS MA

United States Department of Agriculture

Privacy Impact Assessment for the

DA OCP PSD IAS

January 2020

Contact Point
Rick Toothman
IAS System Owner
IAS Branch Chief
202-720-9765

Reviewing Official
Nancy Herbert
DA ISSPM
United States Department of Agriculture
(816)-519-1664

Abstract

The Procurement Services Division (PSD) Integrated Acquisition System (IAS) Major Application (MA) is owned by Departmental Administration (DA) and is operated by Office of Contracting and Procurement (OCP) and hosted at the National Information Technology Center (NITC). The PSD IAS MA is composed of Oracle, PRISM, and iProcurement software in addition to interconnections with Financial Management Services (FMS) Financial Management Modernization Initiative (FMMI), FMMI BI, Forest Service (FS) Document Lookup Tool, GSA Federal Procurement Data System – Next Generation (FPDS-NG), Department of Treasury Invoicing Payment Platform (IPP), and National Information Technology Center (NITC) for hosting. In addition, the eAuthentication application (eAuth) interface is for access control. The overall purpose of the PSD IAS MA is to solve several administrative business issues and to meet federal acquisition requirements. The PSD IAS MA ensures that all procurement 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.

The PIA is conducted to address storage of PII data and to comply with section 208 of the E-Government Act of 2002. This Privacy Impact Analysis has been prepared to update and document the DA OCP PSD IAS MA.

Overview

The IAS MA is owned and operated by OCP-PSD and hosted at NITC. The IAS MA is composed of an Oracle database, PRISM, and iProcurement software applications. IAS MA also has interconnections with FMS FMMI BI, FMS FMMI, FS Document Lookup Tool, GSA FPDS-NG, and Treasury's IPP, and eAuthentication.

The overall purpose of the IAS is to solve several administrative business issues and to meet acquisition requirements.

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?

The IAS MA maintains vendors name, address, e-mail address, SSNs, and TINs.

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

The vendor information in the system is obtained from System for Award Management (SAM) and through FMS-FMMI. SAM is a website, run by GSA, used by entities who need to register to do business with the government, look for opportunities or assistance programs, or report subcontract information. SAM is not part of USDA or in the boundary of the IAS system.

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

The information is being collected for the use of the procurement process.

1.4 How is the information collected?

The information is collected through SAM, the vendor inputs, updates, and provides all data related to its file.

1.5 How will the information be checked for accuracy?

It is the sole responsibility of the vendor using the system to ensure the information obtained is correct and accurate.

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

N/A- It is the responsibility of SAM to define the collection of information.

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

Access to the data in IAS MA is role-based, e-Auth controlled and is done on a business need to know basis to authorized USDA users. The back-end of IAS MA requires predefined USDA Wide Area Network (WAN) channels and NITC VPN access which also conforms to a need to know basis. The databases in which the information is stored are encrypted. IAS is not accessible to public or outside of USDA network.

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.

PIA data is collected and used as necessary to support the procurement process and related financial system functions to include but not limited to purchases, receipts, and payments for goods and services used by the USDA. Only necessary data is collected and stored as a requirement for the functions of the procurement processes. Data is reported to sanctioned Government responsible parties such as FPDS-NG in compliance with mandates from the USDA, Congress and other Federal directives.

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

The IAS MA uses the Oracle APEX tool to analyze data and generate reports from the IAS MA. Web based forms are used in the collection and validation of data during the procurement process. Reports are generated on demand as directed. Data is also reported and conveyed to external sources such as FPDS-NG for reporting. Data extracts are provided to authorize agencies. Excel and other BI tools are used to collect, sample, and analyze data.

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

The IAS MA receives publicly available data from System for Awards Management (SAM) and FMMI. Vendor data from SAM is utilized for procurement processes to include contracts, purchases, and payments. Data is pushed to the financial system (FMMI) for obligation of funds and payment to vendors. Other data such as FAR clauses are pulled into IAS for inclusion in procurement processes as needed. Only authorized sources of data are used to provide external data to IAS.

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 to IAS MA encrypted databases is controlled via role-based user rights and requires USDA WAN connected terminals. Backend access to databases is allowed only via USDA predefined IP addresses and VPN user terminals machines for administrative purposes. Public access to IAS MA is strictly prohibited. A second protective layer in place to user access is USDA wide e-Authentication login mechanisms. All user terminals that connects to IAS are also controlled by two factor authentication mechanism (i.e. pin and LincPass smart badge).

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?

The information is currently being retained indefinitely.

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

The information is currently being retained indefinitely. Data retention period is well over 6 years of retention requirement as per NARA RG-16 manual.

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

An archival strategy has not been implemented for IAS MA. The information is currently being retained indefinitely in the system database. Any risk associated with retention of this data over time is mitigated by limiting access to the data by authorized users who must have proper credentials to access the system. Data stored at the database level is highly encrypted and is not readable in the raw format. Database files on disk are encrypted and not readable at the OS level. Only authorized system administrators with proper credentials are authorized to access the file systems which are non-readable format.

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?

For internal organizations, IAS MA shares information with FMMI and FMMI BI applications. Please refer to the ISA_MOU interconnection agreements.

Information shared with FMMI and FMMI BI is financial and used for the purpose of USDA procurements such as requisitions, awards, payment processing, and vendor information.

4.2 How is the information transmitted or disclosed?

Information transmitted for FMMI and FMMI BI is through a secure VPN tunnel on a USDA network connection.

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.

Internal data/information sharing bears risks if inadequate protective measures are not in place. IAS MA implements Secure Socket Layer (SSL) user access to Web applications, controlled access to databases with front end Web application interfaces, and role-based user access using a second layer of USDA e-Authentication system. All interfaces of IAS MA to other systems such as FMMI are protected behind encrypted channels and are reviewed periodically to enhance security. IAS MA's database highly encrypted.

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 is shared with external organizations such as Treasury's IPP and GSA's FPDS-NG. The information shared with IPP is to provide vendors access and convert their Purchase Orders into electronic invoices. For FPDS-NG, the information shared is to help expedite the processing of data associated with the contracting and procurement processes and fulfill the mandatory requirements of reporting.

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, personally identifiable information outside the Department is compatible with the original collection. IAS does not require a SORN as it is covered under FMMI's SORN, as personally identifiable information is not directly entered into the IAS, but through FMMI. The IAS SORN was requested to retire on November 23, 2012. Please see embedded document which is also located in CSAM under the Status and Archive section.

CTS [DM] IAS
RETIRED SORN FINAl

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

IAS uses secure file transfer protocols (SFTP) and non-persistent encrypted secured channels/connections.

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

Any incident detected, the technical staff will immediately notify their designated counterparts and take steps to determine whether its system has been compromised and take security precautions.

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?

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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.

N/A- SAM is responsible of the information collected.

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?

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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

N/A- SAM is responsible of the information collected.

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?

The IAS user access is controlled by eAuthentication, which the logon process requires the user to enter their user ID and password. PSD documents and follows the Privileged and Non-Privileged User Account Management procedure documents for a user account setup, alteration or de-activation guidelines. All user access is pre-determined and granted strictly on a need-to-know basis.

Privileged User Account Management:

The IAS-201 form is completed on PSD Sharepoint online and digitally signed by the Federal Representative and IAS ISSPM, which the ISSO provides the final signature. The IAS ISSM then enters the request in NITC's access request portal. The Technical Operation Team or Customer Care team sets up all internal, non NITC, PSD accounts. The form is archived within the Sharepoint library for auditing purposes.

There are two types of privileged users, an Internal User (which is used for PSD staff) and External User (who is outside of OCP, i.e. Forest Service Agency).

Privileged users have role-based access, i.e. IAS Developer role, IAS Compliance User role, Help Desk role, IAS Administrator role or IAS Web Developer role.

All users are granted role-based access, which is explained in the "Privileged User Account Management" document.

Non-Privileged User Account Management:

For the Non-Privileged User accounts, access requests are completed online through the online IAS Access Request process and signed by both the Requestor's Supervisor and the IAS Agency Lead. Once the Supervisor and the IAS Agency Lead approve the access request, the user account is systematically created or updated. All access requests, access change requests and approvals are captured in the IAS database for auditability purposes.

All users are granted role-based access, which is explained in the "Non-Privileged User Account Management" document.

8.2 Will Department contractors have access to the system?

Yes

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

Departmental Administration (DA) provides Security Awareness Training (SAT) to all DA users and Protecting Personal Identifiable Information (PII) training.

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

Yes, a Certification & Accreditation giving IAS the full Authority To Operate was conducted on 11/25/2019.

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

The IAS MA system is protected behind NITC's firewall network defense system and has no public access. Access to IAS MA network and operating systems is monitored by NITC data canter. In addition to network protection, IAS MA databases are monitored by an Audit Logging and Monitoring solution, which in real time, monitors and alerts the Security Team of suspicious activities. It also includes but not limited to unknown system administrator level access, failed login attempts, and any unauthorized access that is outside of USDA WAN boundary, table or data deletion attempts. There are a total of over 60 real time auditable events configured to alert IAS MA's Security Team of any suspicious activity. Complete audit logging and monitoring solution implementation information can be found in the Audit Logging and Monitoring Standard Operating Procedures document.

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?

Annual Assessment security control testing is conducted for IAS as well as a full Assessment & Authorization testing every three years. Security control testing affirms that IAS's security posture is up to the high standards set by NIST guidance. This also concludes that audit logging solution and account management processes are performed efficiently to avoid any impact on privacy.

9.1 What type of project is the program or system?

IAS MA is a procurement processing system and is in operational phase.

The IAS MA is composed of an Oracle database, PRISM, and iProcurement software applications. IAS MA also has interconnections with FMS FMMI BI, FMS FMMI, FS Document Lookup Tool, GSA FPDS-NG, and Treasury's IPP, and eAuthentication.

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

No, the IAS MA does not employ technology that might expose privacy act information to unauthorized users.

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?

The IAS MA does not use 3rd party websites and/or applications. The IAS MA has a direct secured data interface/link from through FMMI as it relates to vendor information.

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

N/A - The IAS MA does not use 3rd party websites and/or applications.

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

N/A - The IAS MA does not use 3rd party websites and/or applications.

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?

N/A - The IAS MA does not use 3rd party websites and/or applications.

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

N/A - The IAS MA does not use 3rd party websites and/or applications.

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

N/A - The IAS MA does not use 3rd party websites and/or applications.

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?

N/A - The IAS MA does not use 3rd party websites and/or applications.

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)?

N/A - The IAS MA does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

N/A - The IAS MA does not use 3rd party websites and/or applications.

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

N/A- The IAS MA does not use 3rd party websites and/or applications.

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.

N/A- The IAS MA does not use 3rd party websites and/or applications.

Responsible Officials

X RICHARD TOOTHMAN Digitally signed by RICHARD TOOTHMAN Date: 2020.02.07 12:12:04 -05'00'

RIck Toothman

Rick Toothman
IAS System Owner
IAS Branch Chief
USDA DA Integrated Acquisition System

X NANCY HERBERT Digitally signed by NANCY HERBERT Date: 2020.02.26 10:00:26 -06'00'

Nancy Herbert

Nancy Herbert
DA ISSPM
USDA Departmental Administration

Approval Signature

X CEDRIC BRAGG Digitally signed by CEDRIC BRAGG Date: 2020.02.27 10:37:17 -05'00'

Cedric Bragg

Cedric Bragg
DA OCIO Authorizing Official

USDA Departmental Administration