U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

Introduction

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Integrated Acquisition System (IAS) Major Application (MA)

Office of Contracting and Procurement (OCP)

Departmental Administration Information Technology Office (DAITO)

Date PIA submitted for review:

11/22/2023

Mission Area System/Program Contacts:

Role	Name	E-mail	Phone Number
Mission Area Privacy Officer	Michele Washington	Michele.Washington@usda.gov	202-205-3369
Information System Security Manager	Lisa McFerson	lisa.mcferson@usda.gov	202-720-8599
IAS System Owner/Technical Manager	Marc Taylor	Marc.Taylor@usda.gov	202-207-1249

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 Digital Infrastructure Services Center (DISC).

Overview

Composed of Commercial Off The Shelf (COTS) software products, 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 PSD IAS MA operates under interconnections with Financial Management Services (FMS) Financial Management Modernization Initiative (FMMI), FMMI High-Performance Analytic Appliance (HANA), Forest Service (FS) Document Lookup Tool, FS's Virtual Incident Procurement (VIPR), General Services Administration (GSA) Federal Procurement Data System (FPDS), Department of Treasury Invoicing Payment Platform (IPP), Unison Corporation's Marketplace, Agriculture Maximum (AgMAX), the USDA Enterprise Data Analytics Platform & Toolset (EDAPT) and Digital Infrastructure Services Center (DISC) for hosting from one datacenter location.

The PIA is conducted to address storage of Personal Identifiable Information (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. IAS is currently hosting over 2 million entities comprised of vendors within the system (obtained from SAM.gov) with over 38,000 user entities.

Contents

1 Authorities and Other Requirements 6
1.1 What legal authorities and/or agreements permit the collection of information by the project or system? 6
1.2 Has and Accreditation (A&A) been completed for the system? 6
1.3 What System of Records Notice(s) (SORN(s)) apply to the information? 6
1.4 Is the collection of information covered by the Paperwork Reduction Act? 6
2 Characterization of the Information 6
2.1 What information is collected, used, disseminated, or maintained in the system/program? 7
2.2 What are the sources of the information in the system/program? 8
2.2.1 How is the information collected? 9
2.3 Does the project/program or system use information from commercial sources or publicly available data? If so, explain why this is used. 9
2.4 How will the information be checked for accuracy? How often will it be checked? 9
2.5 Does the system/program use third-party websites? 9
2.5.1 What is the purpose of the use of third-party websites? 9
2.6 PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information. 10
3 Uses of the Information 10
3.1 Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose? 10
3.2 Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results. 11
3.3 PRIVACY IMPACT ANALYSIS: Related to uses of the information. 11
4 Notice 11
4.1 How does the project/program/system provide notice to individuals prior to collection? 11
4.2 What options are available for individuals to consent, decline, or opt out of the project? 12
4.3 PRIVACY IMPACT ANALYSIS: Related to Notice 12
5 Data Retention 12
5.1 What information is retained and for how long? 12
5.2 Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule. 12
5.3 PRIVACY IMPACT ANALYSIS: Related to retention of information. 13
6 Information Sharing 13

6.1 With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted? 13
6.2 PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure. 13
6.3 With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted? 14
6.4 PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure..... 14
7 Redress..... 14
7.1 What are the procedures that allow individuals to gain access to their information? 14
7.2 What are the procedures for correcting inaccurate or erroneous information? 14
7.3 How are individuals notified of the procedures for correcting their information?..... 15
7.4 If no formal redress is provided, what alternatives are available to the individual? 15
7.5 PRIVACY IMPACT ANALYSIS: Related to Redress..... 15
8 Auditing and Accountability 15
8.1 How is the information in the system/project/program secured? 15
8.2 What procedures are in place to determine which users may access the program or system/project, and are they documented? 16
8.3 How does the program review and approve information sharing requirements?..... 17
8.4 Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project? 17

1 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1 What legal authorities and/or agreements permit the collection of information by the project or system?

Chief Financial Officers Act of 1990 (Pub. L. 101–576) is the legal authority that permit the collection of information by this system.

1.2 Has and Accreditation (A&A) been completed for the system?

Yes, a Certification & Accreditation giving PSD IAS MA a full Authority to Operate was initially conducted on 11/25/2019. The PSD IAS MA system has a current ATO and is maintained in the operational environment under continuous monitoring.

1.3 What System of Records Notice(s) (SORN(s)) apply to the information?

Vendor data comes from the system of record, Financial Management Modernization Initiative (FMMI) This is covered under SORN https://www.govinfo.gov/content/pkg/FR-2018-12-31/pdf/2018-28375.pdf.

1.4 Is the collection of information covered by the Paperwork Reduction Act?

Yes. The collection of information is covered by the Paperwork Reduction Act.

2 Characterization of the Information

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

2.1 What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers					
☒	Social Security number (stored as TIN for sole proprietors)			☐	Truncated or Partial Social Security number
☐	Driver's License Number			☐	License Plate Number
☐	Registration Number			☐	File/Case ID Number
☐	Student ID Number			☐	Federal Student Aid Number
☐	Passport number			☐	Alien Registration Number
☐	DOD ID Number			☐	DOD Benefits Number
☐	Employee Identification Number			☐	Professional License Number
☒	Taxpayer Identification Number (or SSN if sole proprietor)			☒	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number			☐	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number			☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number			☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers			☐	Business device identifiers or serial numbers (sole proprietor)
☐	Personal Mobile Number			☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number				
Biographical Information					
☒	Name (including nicknames)	☐	Gender	☒	Business Mailing Address (sole proprietor)
☐	Date of Birth (MM/DD/YY)	☐	Ethnicity	☒	Business Phone or Fax Number (sole proprietor)
☐	Country of Birth	☐	City or County of Birth	☐	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☒	Home Address (potentially if same as business address)	☒	Zip Code	☒	Home Phone or Fax Number (potentially if same as business phone)
☐	Spouse Information	☐	Sexual Orientation	☐	Children Information
☐	Marital Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☐	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)

☐	Employment Information	☒	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☒	Signatures	☐	Weight
Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

2.2 What are the sources of the information in the system/program?

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

2.2.1 How is the information collected?

The information is initially collected through SAM and feeds that data to FMS-FMMI. The vendor inputs, updates, and provides all data related to their file. An interface exists between FMMI and IAS that pulls the data from FMMI transferred thru a secure interface, formatted and programmatically loaded into IAS application.

2.3 Does the project/program or system use information from commercial sources or publicly available data? If so, explain why this is used.

Yes. SAM is a website, run by GSA, used by entities/vendors who need to register to do business with the government, look for opportunities or assistance programs, or report subcontract information. Vendor data from SAM is utilized by IAS MA for procurement processes to include contracts, purchases, and payments.

2.4 How will the information be checked for accuracy? How often will it be checked?

As the initial source of information, the SAM system is responsible for the accuracy of information collected. SAM allows vendors to update their information on demand. SAM requires all vendors to certify that their data is correct annually. The vendor information is feed to IAS through FMMI. FMMI checks the accuracy of the vendor information passed to them from SAM.

2.5 Does the system/program use third-party websites?

Yes

2.5.1 What is the purpose of the use of third-party websites?

Unison Marketplace, supplementing the IAS solution is an online acquisition platform that assists buyers in purchasing the goods and services needed to fulfill their procurement strategies by streamlining the posting of requirements via a simplified Request for Quote (RFQ) process. Marketplace provides the buyer with structured competition information for ease of vendor selection IAS integrates with Marketplace using the Reverse Auction feature.

2.5.1.1 What PII will be made available to the agency though the use of third-party websites?

IAS does not receive data from Unison. No new data elements are created by using this third-party website.

2.6 PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Privacy Risk: Vendor data from SAM is utilized for procurement processes to include contract information, purchases, and payments. IAS MA contains contract sensitive information (including PII data) that is not publicly available and should be protected from non-authorized access during processing, transmission, and storage.

Mitigation: IAS MA implements encryption compliant with USDA's FIPS 140-2 encryption policy for 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 eAuthentication 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 employs encryption and compression for all data elements during storage.

3 Uses of the Information

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

3.1 Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The information is collected initially via GSA's SAM system in which the vendor inputs, updates, and provides all data related to their file. It is the sole responsibility of the vendor using SAM to ensure their information is correct and accurate.
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.

3.2 Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

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 but reports do not include PII data. Data extracts are provided to authorized agencies. Excel and other Business Intelligent tools are used to collect, sample, and analyze data. However, IAS does not produce new or previously unutilized information about an individual.

3.3 PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Privacy Risk: PIA and other sensitive data being accessed by unauthorized users.

Mitigation: Access to IAS MA PIA and sensitive data is controlled via role-based user rights and requires USDA WAN connected terminals to access the application. Backend access to databases is allowed only via USDA predefined IP addresses and VPN user terminals machines for administrative purposes. All IAS data is stored on encrypted SAN devices. 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 connect to IAS are also controlled by two factor authentication mechanism (i.e. pin and LincPass smart badge).

4 Notice

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

4.1 How does the project/program/system provide notice to individuals prior to collection?

SAM provides notice and full disclosure on their website located at:
https://sam.gov/content/about/terms-of-use

4.2 What options are available for individuals to consent, decline, or opt out of the project?

Individuals do not have opportunities to opt out or decline to provide information to SAM. Most of the data collected by the system is related to agency entities which are provided by a company pursuant to applicable laws and regulations rather than directly from users. Additionally, data collected by SAM entities is related to their access and use of the system and is collected through use of the system.

4.3 PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: Proper Notice is not provided prior to data collection.

Mitigation: The SORN is clear, concise, and easily accessible to individuals. It explains what PII is collected, how it is used, and the rights of individuals regarding their data. Additional regular reviews and updated to the SORN are conducted to ensure any changes in practices, legal requirements, or organizational structure are reflected.

5 Data Retention

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

5.1 What information is retained and for how long?

The information is retained per disposition authority DAA-GRS-2013-0003-0001 in which the disposition instruction is to destroy 6 years after final payment or cancellation, but extended retention is authorized if needed for business use. See GENERAL RECORDS SCHEDULE 1.1, item 010.

5.2 Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

The information is currently being retained indefinitely per USDA Records Management policy.

5.3 PRIVACY IMPACT ANALYSIS: Related to retention of information.

Privacy Risk: The information is currently being retained indefinitely in the system database as an archival strategy has not been implemented for IAS MA. This increases the risk of exposure to data that may no longer be necessary for USDA procurement purposes.

Mitigation: Collects only the information necessary for the intended purpose to reduce the risk of exposure and simplify compliance with privacy retention requirements.

6 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1 With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

For internal organizations, IAS MA shares information with Office of the Chief Financial Officer Associate Chief Financial Officer for Shared Services (OCFO ACFO-SS).
Information shared with FMMI and FMMI HANA is financial and used for the purpose of USDA procurements such as requisitions, awards, payment processing, and vendor information.
Information transmitted for FMMI and FMMI HANA is through a secure VPN tunnel on a USDA network connection.

6.2 PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Privacy Risk: Internal data/information sharing bears risks if inadequate protective measures are not in place.

Mitigation: 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.

6.3 With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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. Information is transmitted to external agencies using secure file transfer protocols (SFTP) which is a non-persistent encrypted secured channels/connection.

6.4 PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Privacy Risk: Transmission of PII data elements to external organizations could result in data disclosures if not properly protected and verified accurate.

Mitigation: Risks associated with external sharing and disclosure of PII includes data encryption for data at rest and in transit to protect PII from unauthorized access and ensure encryption keys are managed securely. Following established protocols for sharing PII externally including using other secure channels such as secure file transfer services and limiting the amount of data shared.

7 Redress

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

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

SAM is responsible for the information collected from individuals/vendors. Through SAM.gov vendors can gain access to their information. SAM allows vendors to update their information on demand. SAM requires all vendors to certify that their data is correct annually.

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

Vendors who do business with the USDA submit their information into the GSA's System for Awards Management (SAM), which is subsequently loaded into the Financial Systems. This information includes SSN, TIN, name, address, and bank electronic funds transfer information.

Individuals seeking to contest any information contained in this system of records or its content may submit a request in writing to the Headquarters or Components FOIA Officer, whose contact information can be found at https://www.dm.usda.gov/foia/poc.htm.

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

Systems of Records Notice (SORN) for OCFO-10.

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

SAM is responsible for the information collected from individuals/vendors. Vendors may be notified through the GSA Federal Service Desk website or from calling a live agent.

7.5 PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: SAM is responsible for the information collected from individuals/vendors.

Mitigation: SAM is responsible for mitigating issues related to redress.

8 Auditing and Accountability

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

8.1 How is the information in the system/project/program secured?

The IAS MA system is protected behind DISC's firewall network defense system and has no public access. Access to IAS MA network and operating systems is monitored by the DISC data center. 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.

8.2 What procedures are in place to determine which users may access the program or system/project, 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.

Privileged Users have a higher level of access giving them deeper access to IAS data. Privileged Users access is monitored periodically and adjusted to provide minimum access privileges. Privileges are revoked when access is no longer needed as part of the monitoring process.

All user access is determined and granted strictly on a need-to-know basis. Access is approved and documented as explained below.

Privileged User Account Management:
The IAS-201 form is completed on PSD SharePoint online and digitally signed by the Federal Representative and IAS ISSM. The request is then submitted in in DISC's access request portal. The Technical Operation Team or Customer Care team sets up all internal, non-DISC, 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.