Privacy Impact Assessment for the Integrated Management Administrative Resource Tool System (iMART)

April 2023

Contact Point
Jon Heal*
FAS Application Owner
(202) 720-5728

Reviewing Official
Carol Remmers*
FAS Privacy Officer
(202) 384-4487

*Original Signatures on File in Cyber Security Assessment and Management (CSAM)

Abstract

The Integrated Management Administrative Resources Tool (iMART) provides FAS and the U.S. Department of Agriculture (USDA) Office of the Chief Financial Officer (OCFO) a system that integrates and reconciles multiple financial data sources to support the administrative control of funds, including the reconciliation of financial transactions, and the financial reporting needs to report on global operations.

Overview

The Integrated Management and Resources Tool System (iMART) is a major tool in providing FAS with accurate and detailed data to efficiently manage activities and fiscal operations. iMART data is used to track & locate personnel transactions. iMART consists of sub-systems:

- Integrated Financial Accountability System (iFAS), shall provide FAS with the ability to track, review, approve, and reconcile expenditures at Posts.
- Global Employment Management System (GEMS) shall provide comprehensive employment data for all overseas FAS headquarters employees. Application shall track and locate personnel transactions.

Users of the system include the Office of the Chief Operating Officer (OCOO) Budget Division Employee, Office of Foreign Services Operation (OFSO), Office of Agreements and Scientific Affairs (OASA), Office of trade Program (OTP), Office of Capacity Building and Development (OCDB) and USDA APHIS Employees.

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?

iMART collects the following information:

1) Personnel data - includes name, block/vendor number, address, sex, citizenship, date and place of birth, marital status, and the names and birth dates of eligible family members;
2) Career data - includes education level, college(s) attended, major subjects, skill codes, foreign language training and examination scores, time in class, and time in service;
3) Job history data - includes both current and previous position titles, pay plans, grades, assignment dates, locations, and pending assignment information; and
4) Organizational data - includes organizational hierarchies, accounting information, awards, disciplinary actions, space requirements, etc.

5) Budget & Financial Data – includes Payroll and expenditures at oversea post office.

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

Source of the information is taken from NFC, FMMI, Global Foreign Affairs Compensation System, Department of State Payroll System (EAPS) and Department of State COASTS Data.

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

iMART (Integrated Management Administrative Resource Tool) the information is use for:

- Support the mission of FAS by facilitating the sharing and flow of information (Global Sharing).
- Enterprise platform that automates and synchronizes business processes for HQ & Overseas operations.
- Provide one-stop-shopping for all HR and financial activities.
- Reduce the amount of time required to enter and manipulate data, and gives budget analyst more time to use and analyze it.

1.4 How is the information collected?

Information is collected from the report and/or spreadsheet provide by Global Foreign Affairs Compensation System ,NFC, FMMI, EAPS and COAST.

1.5 How will the information be checked for accuracy?

The data is verified by automated edit checks, reviewed by certified officers.

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

The operation of iMART is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6.

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

iMART collects federal employee's, private citizens and foreign visitor's data included in the records are name, address, birth city, birth country, date of birth, email address, and phone number. PII is collected and must be safeguarded with adequate protections. Data is date and time stamped and only authorized users have access to the data. Data are maintained at DISC in Kansas City and has been assessed and authorized at the Moderate risk category which is sufficient for the data.

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.

iMART Data uses for:

- streamline budgeting and accounting practices across Program Areas
- linkage of financial data to HR data by position and employee
- provide greater accountability of expenditures of funds
- facilitate the complex reconciliation process of financial data from USDA and DOS accounting systems and the multiple payment systems
- reduce the number of auxiliary systems used to process expenditures

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

Standard SQL database access tools are used to input and access the data. The vast majority of data is produced for online viewing; hard copy reports can be produced.

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

No commercial or publicly available data is used.

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

All communications to/from the database is conducted using encryption. Data is also encrypted at rest. The system has been assessed and authorized to operate at the Moderate risk categorization level.

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?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The iMART system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

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

All risk associated with data retention are addressed and have been mitigated in the System Security Plan and the Contingency Plan for the MDA/iMART system.

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?

The information is not shared.

4.2 How is the information transmitted or disclosed?

Information is transmitted by e-mail within USDA.

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

N/A, there is no sharing of the data.

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?

Data is not shared with external organizations. Users have access only to their data using their assigned control number and their registered eAuthentication account.

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.

N/A

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

Sharing of the data produced by the system is outside the scope of the automated system.

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

N/A

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 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, 2019-25020, Integrated Management Administrative Resources Tool System (iMART). USDA/FAS–9.
https://www.federalregister.gov/documents/2019/11/19/2019-25020/privacy- act-of-1974-new-system-of-records

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

Yes

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

N/A

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

N/A

6.5 Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Data collection is done with the active participation of the individual only being notified. Data cannot be collected without them being aware of the collection.

Section 7.0 Access, Redress and Correction

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

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

Individuals can access their data in accordance with the privacy notification.

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

Users can correct any inaccurate data by notifying their FAS Program Area point of contact (POC). The POC will then manually go into iMART to make corrections.

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

Users are given notice of their ability to correct the data when they initially provide the data.

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

Contact information is provided with the privacy notification.

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

With available privacy officer contact information there is minimal privacy risk regarding availability of redress.

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?

All FAS/MDA personnel with access to the system are screened in accordance with USDA personnel procedures and are only allowed access after training and signing specific rules of behavior.

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?

Users are provided annual Information Security Awareness (ISA) training which has a privacy component and users with specific security related positions are provided role based training.

8.4 Has A+A been completed for the system or systems supporting the program?

Yes

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

The MDA/iMART system has undergone the RMF process for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically, iMART system is integrated with USDA eAuthentication software which requires all users of iMART to have an eAuthentication account. iMART software validates the eAuthentication account to confirm the user has access. The technical safeguards are the application level and server level safeguard and security measures (Provided by DISC).

8.6 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?

Privacy risks were identified and mitigated as part of the A&A process for the system. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication account access and operating the system in the secure USDA DISC environment.

Section 9.0 Technology

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

9.1 What type of project is the program or system?

Management Administrative & Financial System

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

iMART does not employ any technology that would raise privacy concerns. Additionally, FAS has an active Configuration Control Board (CCB) which meets every Wednesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for iMART or any MDA component, it would have to be completely vetted by the FAS CCB.

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?

N/A, data is not available through a 3rd party website/application.

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

N/A, data is not available through a 3rd party website/application.

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, data is not available through a 3rd party website/application.

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, data is not available through a 3rd party website/application.

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

N/A, data is not available through a 3rd party website/application.

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, data is not available through a 3rd party website/application.

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, data is not available through a 3rd party website/application.

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, data is not available through a 3rd party website/application.

10.10 Does the system use web measurement and customization technology?

The system does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology? No

10.12 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, data is not available through a 3rd party website/application.