Privacy Impact Assessment
FMMI

Technology, Planning, Architecture, & E-Government

- Version: 1.6
- Date: July 10, 2018
- Prepared for: USDA ACFO-FMS

United States Department of Agriculture

Privacy Impact Assessment for the

Financial Management Modernization Initiative (FMMI)

July 10, 2018

Contact Point
Jeffrey Hoge
Project Manager
USDA ACFO-FMS
202-720-7975

Reviewing Official
Kenneth McDuffie
Information System Security Program Manager
United States Department of Agriculture
USDA ACFO-FMS
504-982-6234

DOCUMENT ADMINISTRATION

Document Revision and History

Revision	Date	Author and Title	Office	Comments
1.0	11/21/2008	Matt O'Brion	Accenture	Initial
2.0	01/21/2009	Matt O'Brion	Accenture	Updates
3.0	08/11/2009	Jerry Chenault	ACFO-FS	Updates
3.2	04/23/2012	Jerry Chenault	ACFO-FS	Updates C&A
3.3	07/23/2013	Scott Roy	ACFO-FS/ISSP	Updates
3.4	09/09/2015	Scott Roy	ACFO-FS/ISSP	Updates
3.5	06/14/2016	Scott Roy/Funsho	SSCD & Securicon	Review and update Rev4.
3.6	11/02/2016	M. Jeffries	ACFO-FS/ISSP	Updated to address USDA Privacy Officer Comments for FMMI CLOUD migration.
4.0	07/10/2018	K Suarez, FMS Security	OCFO-FMS	Update for 2018 Annual and CXO Data Lake Dashboard covering PTA and PIA,

Document Review

Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments
HJ Beckstrom	ASOC Section 508 Representative	02/10/2014	Y	Word and PDF versions of this document are certified Section 508 Compliant as of February 10, 2014.
K. McDuffie	ISSPM	11/02/2016	Y	Reviewed to ensure USDA Privacy Office comments for FMMI CLOUD Migration have been adjudicated
Scott Roy	Alt-ISSPM	07/26/2018	Y	Revisions support annual & CXO Dashboard

Abstract

This Privacy Impact Assessment (PIA) describes the collection, use, processing, and dissemination of personally identifiable information (PII) by the Financial Management Modernization Initiative (FMMI) system. FMMI is USDA's enterprise-wide financial system that provides General Ledger Management, Funds Management, Fund Balance with Treasury, Payment Management, Receivables Management, Cost Management, and Reporting services. This PIA is required by the E-Government Act of 2002 since FMMI processes, stores, and transmits PII data, as identified in the Privacy Threshold Analysis conducted for FMMI.

Overview

System Name: Financial Management Modernization Initiative (FMMI)

USDA Component: Office of the Chief Financial Officer

Purpose: FMMI is USDA's enterprise-wide financial system that provides General Ledger Management, Funds Management, Fund Balance with Treasury, Payment Management, Receivables Management, Cost Management, Grants Management, and Reporting services. USDA agencies and components utilize FMMI for all financial transactions executed by USDA, as well as requests for processing initiated by other Federal agencies.

Description: FMMI is a web-based solution providing access for all USDA financial users. FMMI has interfaces to other financial systems at USDA, such as Payroll, CPAIS, IAS. FMMI

is built on the SAP AG enterprise resource planning (ERP) Central Component 6.0 (ECC) platform – specifically the modules Financials (FI), Controlling (CO), Funds Management (FM), Materials Management (MM), and Sales and Distribution (SD). In addition, FMMI utilizes SAP Business Intelligence for Reporting, SAP Customer Relationship Management (CRM) for grants management, SAP Process Integration for interfaces to other systems, and SAP Governance, Risk, and Compliance for ensuring Segregation of Duties controls are enforced. Enhanced functionality is provided through the use of custom RICEFW objects to supplement the standard SAP ERP software. RICEFW Objects have been developed for reports, interfaces, conversions, enhancements, forms, and workflows. The Pega application component with in the FMMI SAP CRM solution that allows grantees to search for grant opportunities, apply for grant opportunities, view agreement details, file claims, and receive status updates.

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?

FMMI contains USDA employee data, government and commercial vendor data, agency budget execution data, procurement data, financial data, and program and administrative information. Information types include Accounting, Budget Formulation, Cost Accounting/Performance Measurement, Funds Control, Information Security, Payments, Grants Management, and Personal Identity and Authentication.

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

The two primary sources for data in FMMI are conversion from legacy systems and interfaces with external systems. Systems that will provide data for conversion to FMMI include:

Systems that provide data to FMMI through interfaces include:

Government Online Accounting Link System (GOALS) II, Automatic Standard Application for Payment (ASAP), Invoice Processing Platform

Financial Statements Data Warehouse (FSDW)

Automated Cash Reconciliation Worksheet (ACRWS)

Reporting of IPAC Transaction for Agriculture (RITA)

Micellaneous Income System (MINC)

Program Loan Accounting

Marketing and Regulatory Program

Health and Human Services

Grants and Awards, Grants.gov

Forest Service Candidate Systems

Ameresco / MetTel

Cooperative Research, Education and Extension Mgt.

SmartPay 2 □

Corporate Property Automated Information System (CPAIS) □

Integrated Acquisition System (IAS) □

Payroll/Personal System

Administrative and Billings and Collections System

LockBoxes (US Bank and Citi Bank)

ETS2 – Government Travel

mLINQs (moveLINQ-USDA)

System and Award Management (SAM)

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

This data is used for financial planning and management, to make payments, and for reporting to government agencies, such as Treasury and the Office of Management and Budget for budget execution, cash disbursements, and other financial obligations.

1.4 How is the information collected?

Data is collected from all USDA agencies' accounting and budget execution transactions, or directly entered into FMMI by users assigned to financial administration roles. Additionally, Pega users enter information regarding grants and agreements with grantees.

1.5 How will the information be checked for accuracy?

Data received by FMMI requires a highly concise format consistent with other USDA financial systems. Data not in the proper format will trigger an alert for auditors to examine. Data that is properly formatted but that contains erroneous numbers, misspelling, etc., will fail automated checks applied by the system. These failures will also trigger an alert for auditors to examine. External agencies implement additional checks for accuracy, including transaction integrity checksums. Counts of processed records are checked against expected values to ensure that all transactional processes have been completed.

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

Legal Authorities:

5 U.S.C. Section 301, Departmental regulations.

5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence.

26 U.S.C. Section 6011, General requirement of return, statement, or list.

26 U.S.C Section 6109, Identifying Numbers.

31 U.S.C. 3711 through 3719, Claims of the United States Government.

31 U.S.C. Money and Finance; Chief Financial Officers Act of 1990.-

FMMI operates under the following System Of Record Notices:

USDA/OCFO – 10, "Financial Systems"

USDA/OP – 1, "Personnel and Payroll System for USDA Employees"

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

Privacy risks identified include unauthorized access to individual or group PII data, or aggregation of non-specific data that could be used for malicious intentions, for the purposes of fraud, extortion, loss of public trust, or other abuses. FMMI was accredited in 2009, following a thorough assessment of the implemented security controls and their effectiveness. Since that time, additional security control measures have been implemented to further protect PII data processed and stored within the system. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view information about others can do so. The following security controls are also utilized and continuously reviewed to ensure a high level of protection for the FMMI system and associated data:

Annual Vulnerability Assessments □

Real-time Intrusion Detection □

Firewall Monitoring and Alerting □

Active Directory Monitoring □

Database Monitoring □

Site Protection Monitoring □

Identity Management Monitoring □

Monthly Virus and Compliance Scans □

Active Host Virus Monitoring

All systems interacting with FMMI are required to have appropriate security controls. This includes the VFC hosting facility, client systems accessing FMMI, and integrated applications supported and managed by ACFO-FMS. Integrated target systems must have a valid ATO in effect and memorandum of understanding (MOU) to ensure that information is only used in the intended manner, and a signed Interconnection Security Agreement (ISA) to ensure data are passed securely. Please refer to Sections 4.0 and 5.0 below for more information on the security precautions that are taken before a target system integrates with the FMMI system.

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.

This data is used for financial planning and management, to make payments, the awarding of grants, and for reporting to government agencies, such as Treasury and the Office of Management and Budget for budget execution, cash disbursements, and other financial obligations.

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

FMMI utilizes the SAP Governance, Risk, and Compliance (GRC) Access Control product to supplement the core security provided by SAP and Pega. Specifically, GRC provides robust functionality to ensure that segregation of duty (SoD) conflicts are not introduced into

the system. GRC is configured to run in preventative mode to prevent these conflicts from occurring. The following components are implemented within GRC Access Control to handle access provisioning and SoD conflicts:

Access Risk Analysis (ARA), Emergency Access Management (EAM), and Access Request Management (ARM). The Access Control tool handles FMMI provisioning across ECC, BI, Portal, CRM, Solution Manager, PI and the GRC system for end users and the project support team members. FMMI Portal is the single Point of Entry for all FMMI applications including GRC Access Control.

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

Not applicable. FMMI does not use commercial or publicly available information.

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.

FMMI is protected via USDA eAuthentication which serves as a gateway for accessing the system. Information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary.

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?

FMMI data is retained by ACFO-FMS for at least 6 years and 3 months. Different data types have different retention periods.

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

Yes. Records are retained in accordance with NARA policies, USDA DR 3080-001, Records Management, USDA DR-3090, Litigation Retention Policy for Documentary Materials including Electronically Stored Information, et al.

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

ACFO-FMS has determined that data retention periods and practices are adequate to safeguard PII while ensuring that mission critical data is available to support system restoration in the event of unplanned outages

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 FMMI system, operated on behalf of the USDA by ACFO-FMS, shares information with other USDA systems operated by the Office of Procurement and Property Management, the National Finance Center, and the Research, Education and Economics mission within the Office of the Chief Scientist. PII data relevant to financial transaction processing is shared with these internal USDA organizations. Information may be shared with senior leadership across USDA through a series of Tableau dashboards and reports for the purpose of promoting data-driven decisions. The information shared will span data from different various administrative domains including IT, Finance, HR, Property, Operations, Homeland Security, and Property and Fleet.

4.2 How is the information transmitted or disclosed?

Information is shared almost exclusively via electronic file transfer. Security measures implemented to protect the electronic sharing of information amongst USDA agencies are described in the FMMI Interconnection Security Agreements. Manual data sharing (CD, hardcopy, etc.) is permitted only in rare and special circumstances. The information will be transmitted to the USDA Data Lake via secure file transfer methods such as SFTP, API, and Web Service. Once in the USDA Data Lake, data will be shared via a series of Tableau dashboards.

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.

There are no significant risks associated with the internal sharing of PII data amongst USDA agencies. All personnel accessing FMMI PII data are cleared and trained annually on the proper

handling and protection of PII data. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary. Risk when sharing within USDA is considered low-moderate. Should data sharing include sources of the network, encryption protocols ensure PII is not inadvertently shared in an unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with a need-to-know through the use of internal, granular governance process. Dissemination of information is governed by internal policy. Access to information is monitored, tracked, logged and audited using tools such a Cloudera Navigator and Cloudera Manager.

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?

FMMI financial and PII data is shared with the following organizations, for the purpose of accurate accounting transactions: Department of the Treasury, for monetary disbursements

Internal Revenue Service, for tax reporting and collection.

Office of Management and Budget, for USDA financial reporting.

Grants data is shared with external grantees for the purpose of awarding and status

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.

External sharing of PII data is compatible with the original collection. Routine uses of the information is covered in SORN OCFO – 10, Financial Systems

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

Information is shared almost exclusively via electronic file transfer. Manual data sharing (CD, hardcopy, etc.) is permitted only in rare and special circumstances. All FMMI interconnections are safeguarded through security measures defined within established Memorandum of

Understanding and/or Interconnection Security Agreements. Security controls applied to system interconnections are regularly assessed to verify and validate that security protections are operating as intended.

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

There are no significant risks associated with the external sharing of PII data amongst USDA agencies. All personnel accessing FMMI PII data are cleared and trained annually on the proper handling and protection of PII data. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary.

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?

U.S. Government intention to collect PII data is declared in various System of Record Notices made publicly available within the U.S. Federal Register, as well as in the Privacy Act, and at data collection points throughout the Federal government. Individuals who enter their own PII data are notified of their rights and protections under the Privacy Act before providing information via those collection points, which are outside the scope of control of USDA ACFO-FMS. FMMI does not directly request PII data from individuals as part of its routine operations.

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

Individuals are given the opportunity and the right to decline provision, based upon protections and limitations in various U.S. Regulations, Acts, guidelines, policies, etc., at the myriad points of collection. FMMI does not directly request PII data from individuals as part of its routine operations.

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

Individuals consent to particular uses of the information at the time of provision. Grievances involving consent and unauthorized use of the information can be addressed to the collecting

Government agency, to agencies listed within applicable System of Record notices, or through other legal means.

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.

Notice is provided at the time of collection. The mechanism for notification may vary depending on the Government agency or commercial entity that manages the collection point. No data is collected by FMMI itself. Individuals seeking mitigation action can contact the USDA Office of the Chief Financial Officer directly, or the Government agency or commercial entity that collected the information. Section

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 may obtain information regarding the procedures for gaining access to their own records contained within FMMI by submitting a request to the Privacy Act Officer, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and all letters contained therein, should bear the words "Privacy Act Request." A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s).

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

Procedures for contesting records are the same as procedures for record access in section 7.1 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

Notification is provided in the system of records notice available in the Federal Register. Procedures for contesting records are the same as procedures for record access in section 7.1

above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

If formal redress is not possible after contacting USDA in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited to, filing civil and/or criminal complaint

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

Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records Notice posted in the U.S. Federal Register. Internal employees may also contact their respective Human Resources and/or Privacy Office representative for further assistance.

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?

Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records Notice posted in the U.S. Federal Register. Internal employees may also contact their respective Human Resources and/or Privacy Office representative for further assistance.

8.2 Will Department contractors have access to the system?

Yes, there are USDA contractors that have access to FMMI.

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

All USDA employees and contractors receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users are required to take additional, more detailed security training commensurate with their access permissions.

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

Certification and accreditation was last completed for FMMI on 11/10/2016.

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

FMMI logs all accesses to sensitive PII data. These logs are reviewed monthly for indications of misuse. The Virtustream Federal Cloud (VFC)hosting environment provided real-time monitoring of networked connections and data flow. User accounts are re-authorized annually for continued need and applicability.

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?

There are no significant risks associated with the sharing of PII data amongst USDA agencies or external agencies with which an ISA has been established. All personnel accessing FMMI PII data are cleared and trained annually on the proper handling and protection of PII data.

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?

FMMI is considered an ACFO-FMS Major Application and a Cloud-based system.

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

FMMI does not use technology that would prompt an increase in concern regarding privacy protection. FMMI components are commercial off-the-shelf products that all benefit from robust security configurations developed by both government and industry.

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. The FMMI System Owner and the ISSPM have reviewed both OMB M-10-22 and M-10-23.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not applicable. FMMI does not utilize any 3rd party websites or Software-as-a-Service applications. All FMMI components are hosted and provided by USDA components, with data sharing only with other Federal agencies.

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

Not applicable.

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

Not applicable.

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?

Not applicable.

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

Not applicable.

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

Not applicable.

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?

Not applicable.

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)?

Not applicable.

10.10 Does the system use web measurement and customization technology?

Not applicable.

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?

Not applicable.

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.

Not applicable.

Responsible Officials

Jeffrey Hoge

Project Manager

ACFO-FMS

United States Department of Agriculture

Approval Signature

GREGORY ROY Digitally signed by GREGORY ROY
Date: 2018.08.02 07:04:13 -05'00'

Gregory S. Roy
Information Systems Security Officer
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture

KENNETH MCDUFFIE Digitally signed by KENNETH MCDUFFIE
Date: 2018.08.02 08:15:15 -05'00'

Kenneth McDuffie
Information Systems Security Program Manager
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture

MATTHEW LEGER Digitally signed by MATTHEW LEGER
Date: 2018.08.02 13:16:34 -04'00'

Matthew Leger
Acting Information Systems Owner
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture