Privacy Impact Assessment
APHIS Cost Management System

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: August 30
- Prepared for: Marketing and Regulatory Programs

Privacy Impact Assessment for the

APHIS Cost Management System

August 30, 2022

Contact Point

Kelly Stiles
Acting System Owner
MRP-APHIS-FNANCL MGMT DIV

Reviewing Official

Tonya G. Woods
MRP-APHIS Privacy Act Officer
(301)851-4076

Abstract

The APHIS Cost Management System (ACMS) is a Major Application used by the Animal and Plant Health Inspection Service (APHIS) to provide a relevant Status of Funds for all levels of the agency. It also tracks information on agreements and grants for the Marketing and Regulatory Programs (MRP) and inactive Unliquidated Obligations oversight. This system is used by APHIS' financial analysts and MRP agreement specialists. This Privacy Impact Assessment (PIA) is being completed following the Privacy Threshold Analysis (PTA) conclusion requiring a PIA for ACMS to meet federal privacy compliance requirements.

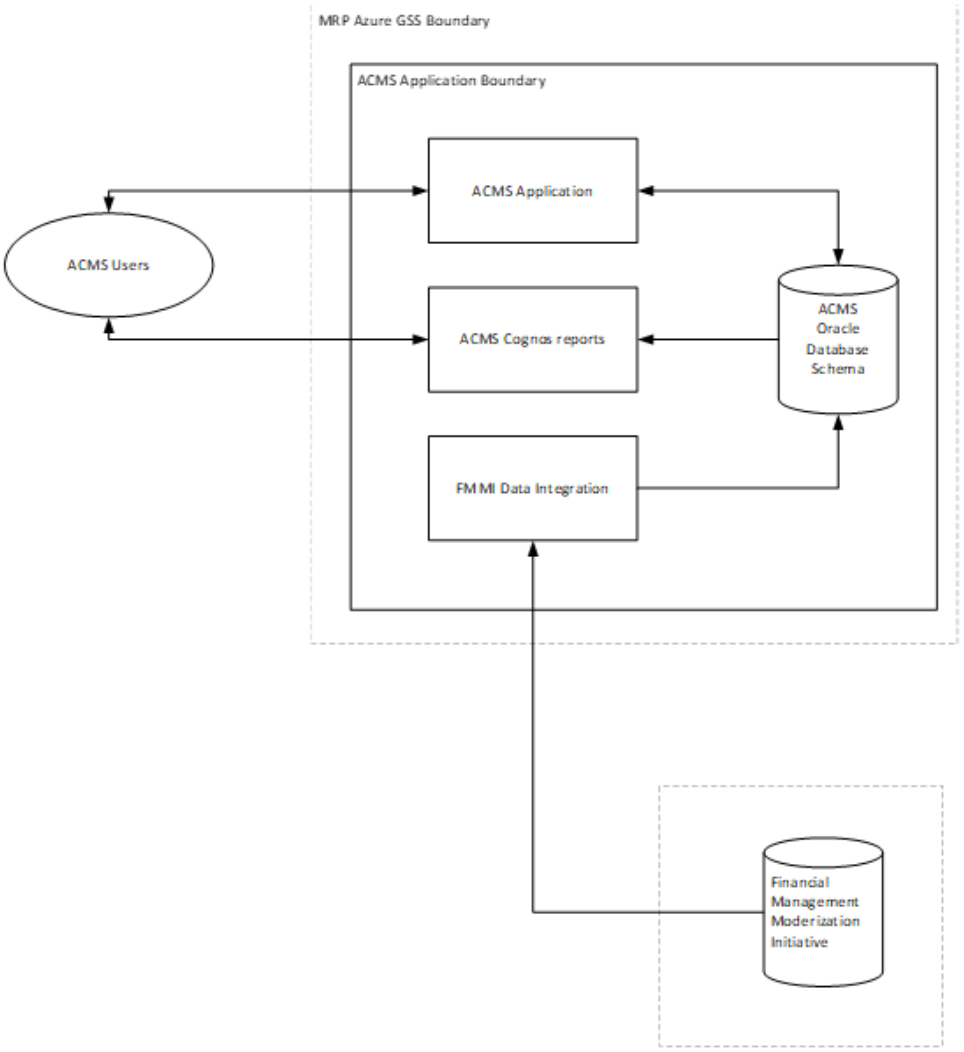
Overview

The APHIS Cost Management System (ACMS) is owned by the Animal and Plant Health Inspection Service (APHIS) Marketing and Regulatory Programs Business Services (MRPBS). The MRPBS Financial Management Division (FMD) is tasked with maintaining an Agency Status of Funds for APHIS. ACMS provides the functionality to perform these tasks.

ACMS provides APHIS a relevant status of funds and is able to substantiate it using a consistent well-defined process that is flexible for all levels of the organization at any time during a financial cycle. ACMS is a tool to track, reconcile, adjust, and analyze the balance of allocations through year end for any financially interested APHIS party. This process is known as status of funds processing. The ACMS accomplishes this status of funds processing by tracking planned and committed expenses as this data is reconciled to matching obligation from the official accounting system.

ACMS was granted Authority to Operate (ATO) on July 23, 2020, which is valid until July 23, 2023.

ACMS Process Data Flow Diagram



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?

- ACMS collects PII related to USDA employees, Contractors or other entities working on behalf of USDA, the general public, farmers, ranchers, and producers.

  The type of PII present in ACMS includes:

- Business names (such as farmers, ranchers and producers), addresses and phone numbers related to APHIS Agreements, Grants and Indemnities.

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

Sources of the data are Animal and Plant Health Inspection Service (APHIS) and Agriculture Marketing Service (AMS) employees, and the USDA Financial Management Modernization Initiative (FMMI) system.

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

The PII provides context to the financial data collected from FMMI and agreement/grant tracking.

1.4 How is the information collected?

APHIS transfers the PII data from the FMMI system using an SFTP transient connection for the Status of Funds module. For Agreements, all data is based on what resides in FMMI and ezFedGrants records. Agreement specialists manually input select data points (name and address) from FMMI and into ACMS for the purpose of tracking and reporting in compliance with the Transparency Act (FFATA).

1.5 How will the information be checked for accuracy?

Data is received from FMMI and checked through the ACMS for accuracy. If data is incorrect, the FMMI system is updated. ACMS is a reporting tool for FMMI data.

The accuracy of the information in the Agreement is collected directly from the Agreement document or Agreement data from FMMI and checked by the user during data entry.

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

ACMS has an interconnection security agreement with FMMI. The initial collection takes place within FMMI and therefore the FMMI System Owner has responsibility for additional agreements around collection and notice.

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 include the unintentional dissemination of the received and stored PII.

The privacy rights of the customers and employees will be protected by USDA, APHIS management.

- All access to the system is limited by USDA eAuthentication credentials.
- Application limits the access to relevant information and prevents access to unauthorized information.

Data is secured by means of encryption and access control. Access is controlled by:

- USDA eAuthentication credentials
- User Role Assignments
- Application Role Assignments

As part of the access control process, all users are required to take annual Information Security Awareness Training that educates them on the properly handling and protection of PII data. This is a requires for both initial and continued access to the 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.

The information is used by APHIS financial analysts to track and manage estimated and actual obligation data in order to develop a Status of Funds and review inactive unliquidated obligations for all levels of the agency. Agreement information is used by APHIS and AMS agreement specialists to track and manage grants in order to report this information to OMB under FFATA.

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

The ACMS application provides the capability to reconcile estimated obligations and actual obligations through the creation of ledgers. These ledgers are compared against budget authority data in order to produce a Status of Funds. The application also provides the capability to track and manage inactive unliquidated obligations, agreements/grants within APHIS and AMS.

ACMS uses IBM Cognos Analytics to provide reporting to ACMS users.

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

Not Applicable. ACMS does not use commercial or public data.

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.

All ACMS privilege users are required to complete a Financial Systems Access Request Form to request access to the system. ACMS contains information to report user status as active or inactive, as well as the last activity date. The activity log is reviewed annually to mark users as inactive if they have not used the system in the previous 12 months.

In addition, data is secured by means of encryption and access control. Access is controlled by:

- USDA eAuthentication credentials
- User Role Assignments
- Application Role Assignments
- APHIS tracks changes to the data to include, who changed the data and when the data was changed.

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?

Status of funds module: Destroy when final report is completed or when printouts cease to have administrative value, but no later than 3 years, whichever is earlier

Agreements module: Destroy 5 years after close of fiscal year.

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

Yes, records schedule number: DAA-0463-2017-0002. The retention period was approved as of 7/18/2018.

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

Risks associated with data retention are minimal, the major risk being the possibility of the data being accessed by unauthorized personnel. This risk is minimized by the control methods outlined in Section 2.4

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?

ACMS receives information from FMMI in a one-way connection. No information is shared by ACMS to any other organization or system.

4.2 How is the information transmitted or disclosed?

N/A

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.

N/A

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 contained within this application is not shared with Non-USDA organizations.

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.

Not Applicable.

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

Not Applicable.

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

Not applicable.

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. The data included in the ACMS system is covered by OFCO-10 SORN, which can be found here: (2018-28375.pdf (govinfo.gov))

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

Not Applicable: ACMS does not collect PII. All PII received by the system comes from two systems: FMMI and EzFedGrants, both of which are operated and maintained by USDA-OFCO. As such, OFCO-10 SORN covers this data.

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

Not Applicable: addressed by bullet 6.2

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

Not Applicable: addressed by bullet 6.2

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

Not Applicable: addressed by bullet 6.2

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?

Any individual may obtain information about the information in the system that pertains to them. Requests for hard copies of the records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in questions, any other pertinent information to help identify the file and verification of identity as described in 7 CFR, Part 1, Subpart G §1.113(e). All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

Any PII information obtained from the FMMI system would be subject to the applicable procedures to allow individuals to gain access to their FMMI information. Note that the applicable procedures to allow individuals to gain access to their FMMI information are maintained outside the accreditation boundary of this application.

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

Any PII information obtained from the FMMI system would be subject to the applicable procedures to allow individuals to gain access to their FMMI information. Note that the applicable procedures to allow individuals to gain access to their FMMI information are maintained outside the accreditation boundary of this application.

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

Refer to the OCIO-10 SORN regarding all privacy data present in ACMS. Data is received from FMMI which is the authoritative data source.

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

Refer to the OCIO-10 SORN regarding all privacy data present in ACMS. Not applicable.

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 as redress is provided through FMMI and EzFedGrants.

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?

Access controls for ACMS is described in Section 2.4. The processes utilized are well-established and documented.

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?

All users are required to take annual Information Security Awareness training, which includes training on proper handling of PII.

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

Yes. The system received an Approval to Operate (ATO) on 07/23/2020. The FISMA A&A will be conducted on an annual basis, until the ATO expires on 07/23/2023.

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

APHIS conducts continuous monitoring for the system to ensure the technical safeguards are in place. Additionally, the system provides technical safeguards to prevent misuse of data including:

- Confidentiality : Encryption is implemented to secure data at rest and in transit for the application (HTTPS and database encryption).
- Access Control : Role/feature based access is used to ensure staff only receives access to limited data.
- Authentication : Access to system and session timeout is implemented for this application (by eAuthentication)
- Audit : Logging is implemented for this application (date/time of the last record update, user that last updated the record).

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?

This system does not share information, but rather only receives data. The interconnection with FMMI is conducted in specific ways to mitigate any privacy risks. There is no direct connection between the two systems. Each night, FMMI places a read-only report on a secure SFTP site. This report data is then processed into ACMS.

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?

A cost management system.

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

No.

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"?

The ISSPM and system owner have reviewed the OMB memorandums listed above.

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

Not Applicable. The system does not use of 3rd party websites and/or applications.

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?

No, 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 all uses of web measurement and customization technology?

Not Applicable.

10.12 <u>Privacy Impact Analysis</u>: 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.

Agency Responsible Officials

SUSAN MURPHY
Digitally signed by SUSAN MURPHY
Date: 2023.11.21 12:29:27 -05'00'

Kelly Stiles
Acting System Owner
Animal and Plant Health Inspection Service /
Marketing and Regulatory Programs
United States Department of Agriculture

Date

Agency Approval Signature

Janelle Jordan
Digitally signed by Janelle Jordan
Date: 2023.11.21 17:26:36 -05'00'

Tonya Woods
Privacy Act Officer (PAO)
Marketing and Regulatory Programs
United States Department of Agriculture

Date

ANGELA COLE
Digitally signed by ANGELA COLE
Date: 2023.11.21 17:54:28 -05'00'

Angela Cole
Chief Privacy Officer/Deputy Assistant Chief Information Security Officer
Marketing and Regulatory Programs
United States Department of Agriculture

Date