Privacy Impact Assessment

APHIS Cost Management System (ACMS)

Revision: 1.1

Animal and Plant Health Inspection Service (APHIS)

Date: June 2009

Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only

USDA PRIVACY IMPACT ASSESSMENT FOR ACMS

Agency: Animal and Plant Health Inspection Service (APHIS)

System Name: APHIS Cost Management System (ACMS)

System Type: ☒ **Major Application**
☐ **General Support System**
☐ **Non-major Application**

System Categorization (per FIPS 199): ☐ **High**
☒ **Moderate**
☐ **Low**

Description of the System:

The 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. The 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.

Who owns this system?

U.S. Department of Agriculture (USDA) Marketing and Regulatory Programs (MRP)
APHIS Marketing and Regulatory Program Business Services (MRPBS)
Stacye L. Teachman
System Owner/Supervisory Budget Analyst
MRPBS, FMD, BEST
4700 River Road
Riverdale, MD 20737
(301) 734-8251
Stacye.L.Teachman@aphis.usda.gov

Who is the security contact for this system?

Michael Fuchs
Information System Security Manager
APHIS MRPBS ITD
4700 River Road
Riverdale, MD 20737
(301) 851-2527
Michael.Fuchs@aphis.usda.gov

Who completed this document?

Prepared in December 2007 by:
COACT, Inc.
9140 Guildford Road, Suite N
Columbia, MD 21046
(301) 498-0150

Revised in June 2009 by:
Brian Bowman
ACMS Project Manager
USDA MRPBS ITD
4700 River Road Unit 103
Riverdale, MD 20737
(301) 851-2516

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**YES**	**YES**
Social Security Number	**YES**	**YES**
Telephone Number	**YES**	**YES**
Email address	**NO**	**YES**
Street address	**YES**	**YES**
Financial data	**YES**	**YES**
Health data	**NO**	**NO**
Biometric data	**NO**	**NO**
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]		
Are social security numbers embedded in any field?	**YES**	**YES**
Is any portion of a social security numbers used?	**YES**	**YES**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**YES**	**YES**

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

There will be two types of data that will be used in the system, APHIS employee data and other data. These two types of data are described below:

***Employee Data**: USDA APHIS users use the ACMS to track and analyze daily spending for the agency as this data is reconciled against obligations obtained from the Foundation Financial Information System (FFIS). Employee information stored includes: User ID, e-Authentication ID, Federal Data Warehouse (FDW) User ID, First Name, Middle Name, Last Name, Email, and Organization(s).*

Additionally, ACMS users enter Employee Salary Projection data for each employee. This allows them to provide estimated salary spending over one or more pay periods. Data collected for employees entered into ACMS include: First Name, Middle Name, Last Name, Social Security Number, Employee Type, Location, Job Title, Pay Plan, Grade, Step, Locality, Benefits Plan, Appointment Type, Work Schedule, Hours per Pay Period, Allowances; and Estimates per pay period on Salary, Benefits, Overtime, Other Pay.

***Other Data**: ACMS users enter general information into the application regarding other types of individuals providing a means of identifying and/or contacting the individual or entity. This includes data for Grants, Cooperative Agreements and Indemnity payments. All of this data is required to be captured by the Federal Funding Accountability and Transparency Act (FFATA) of 2006. The data includes: (a) <u>Agreement Contact Information</u>: Contact Type, First Name, Middle Name, Last Name, Phone Number; (b) <u>Agreement Cooperator Information</u>: Name, City, State, Country, Cooperator Type, and Minority Flag. Vendor Code (possibly SSN); and (c) <u>Primary Location of Performance Information</u>: Address, City, State, Zip code, and Congressional District.*

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

☒ Yes
☐ No

The data is relevant and necessary. The ACMS was developed to replace several subsystems that did not have the ability to compute real-time expenses in any given year. This system adds value by enabling APHIS to manage funds allocated by US Congress and helps them determine how much of the funds have been spent, how much of the funds remain and how much of the funds have been spent relating to strategic goals of the agency. In addition, FFATA requires the capture of information about Agency agreements for mandated reporting to OMB.

5. Sources of the data in the system.

5.1. What data is being collected from the customer?

Customer: Information collected on the SF-424, Application for Federal Assistance. This information is used to establish Agreements between the Agency and the requesting entity. Information is reviewed by ACMS users who enter the appropriate data into ACMS.

Employee: The application user's information will be provided by e-Authentication data, the FDW and direct entry by the user. This information is reviewed by the user in a formal request for access to the system. Employee data within the Employee Salary Projection module will be provided via direct entry by managers who are authenticated ACMS users.

Other: Direct entry by an ACMS user.

5.2. What USDA agencies are providing data for use in the system?

Administrative data will be obtained from the National Finance Center's (NFC) FDW.

USDA eAuthentication Service will provide some user specific data such as the unique eAuthentication User ID, first name, last name and email address. Users will review name and email address for accuracy.

5.3. What state and local agencies are providing data for use in the system?

State or Local Agencies apply for Federal Assistance through the SF-424. The data collected on this form is stored in ACMS. They are customers receiving the Federal assistance and their information is stored.

5.4. From what other third party sources is data being collected?
No third party services are used.

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

☒ Yes
□ No. If NO, go to question 7

Although data will not be collected from sources external to the USDA, data from internal sources will be used such as information from the FFIS and FDW, which are National Finance Center (NFC) systems.

6.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

Data collected on the SF-424 form will be verified during the Agreement approval process which entails the Agreement Specialist reviewing the data provided on the forms for accuracy.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Most of the data within ACMS originates from other systems for reporting and cost management purposes. This information is deemed to have undergone validation checks, checks for accuracy and completeness at the originating source (i.e. FFIS, FDW, and EMRS).

Users entering information into the system must have a valid APHIS e-Authentication ID, an FDW user ID, and access privileges granted by a system administrator for system use.

Other information that is entered consists of agreement contact or agreement cooperator information that may be received via hardcopy document or over the telephone from other USDA employees. This information is double checked from hardcopy document upon being entered and/or validated against existing information in other external supporting systems. Such information includes:

Agreement Contact--Contact Type, First Name, Middle Name, Last Name, Phone Number; Agreement Cooperator--Name, City, State, Country, Cooperator Type, Minority Flag, and Vendor Code (possibly SSN); Primary Location of Performance--Address, City, State, Zip code, and Congressional District

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Information from customers that is entered consists of agreement contact or agreement cooperator information that is received via hardcopy document. This information is double checked from hardcopy document upon being entered and/or validated against existing information in other external supporting systems. Such information includes:

Agreement Contact--Contact Type, First Name, Middle Name, Last Name, Phone Number; Agreement Cooperator--Name, City, State, Country, Cooperator Type, Minority Flag, and Vendor Code (possibly SSN); Primary Location of Performance--Address, City, State, Zip code, and Congressional District

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected? *The principal purpose of information contained with the ACMS application is to afford the agency the capability to track and analyze daily spending for the agency as this data is reconciled against obligations obtained from FFIS. In addition, data required by FFATA will be reported to OMB.*

8. Will the data be used for any other purpose?

□ Yes
☒ No. If NO, go to question 9

8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

☒ Yes
□ No

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

□ Yes
☒ No. If NO, go to question 11

10.1. Will the new data be placed in the individual's record (customer or employee)?

□ Yes
□ No

10.2. Can the system make determinations about customers or employees that would not be possible without the new data?

□ Yes
□ No

10.3. How will the new data be verified for relevance and accuracy?

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected? *There are no identifiable routine uses of information within ACMS. The information is obtained from other source only for reconciliatory purposes and is only reviewed for said purposes. Information for FFATA reporting purposes is collected through the SF-424 and customers are notified of the routine uses through that vehicle.*

12. Will the data be used for any other uses (routine or otherwise)?

□ Yes
☒ No. If NO, go to question 13

12.1. What are the other uses?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

☒ Yes
□ No. If NO, go to question 14

13.1. What controls are in place to protect the data and prevent unauthorized access?

All access is controlled through the FDW user ID which limits the financial data which the user can access. More detail on the controls that are in place to protect the data from unauthorized use are specifically defined in the ACMS System Security Plan.

14. Are processes being consolidated?

☒ Yes
□ No. If NO, go to question 15

14.1. What controls are in place to protect the data and prevent unauthorized access?

The ACMS was developed to eliminate the processes found in several legacy systems. Security safeguards have been incorporated into the system to restrict access based on need-to-know concepts with further restrictions to support least privileges concepts. These controls are detailed in the ACMS System Security Plan but the architecture includes mechanisms for identification and authentication, as well as authorization to only those organizational identifiers that the users have been authorized to review. FFATA reporting is protected by using a secure encrypted data transmission line. Risk and threats to the system are specifically addressed in the ACMS Risk Assessment Report.

DATA RETENTION

15. Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 16

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

15.2. What are the procedures for purging the data at the end of the retention period?

15.3. Where are these procedures documented?

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
Data relates to a particular business. Business transactions are recorded and reconciled and remain as historic documentation of a completed event. It does not undergo changes or further modifications over time unless there is a subsequent business transaction conducted.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
☐ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

☒ Yes
□ No. If NO, go to question 19

18.1. How will the data be used by the other agency?

OMB will present the data collected to process Grants, Indemnity Payments and Cooperative Agreements on a public web site as required by Federal Funding Accountability and Transparency Act (FFATA) of 2006. This data will include: (a) Agreement Contact Information--Contact Type, First Name, Middle Name, Last Name, Phone Number; (b) Agreement Cooperator Information--Name, City, State, Country, Cooperator Type, and Minority Flag. Vendor Code (possibly SSN); Primary Location of Performance Information--Address, City, State, Zip code, and Congressional District.

18.2. Who is responsible for assuring the other agency properly uses the data?

OMB is responsible for the proper use of the data collected under FFATA from all of the federal agencies.

19. Is the data transmitted to another agency or an independent site?

☒ Yes
□ No. If NO, go to question 20

19.1. Is there an appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

Yes. The agreement is with the USDA Chief Information Office.

20. Is the system operated in more than one site?

□ Yes
☒ No. If NO, go to question 21

20.1. How will consistent use of the system and data be maintained in all sites?

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?
System administrators, developers, and any APHIS approved ACMS user will have access to the data in the system.

22. How will user access to the data be determined?
User access will only be granted to USDA employees having a valid need to access data in the system. This need will be based on job functions and approval by appropriate managerial staff. Requests must be submitted and approved prior to system administrators adding or allowing access.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

☒ Yes
☐ No

NOTE: Procedures, controls, and responsibilities regarding user access are documented within our Security Administrator Procedures guide and ACMS User Manual.

23. How will user access to the data be restricted?
Users do not have direct access to databases and data. All access is through application systems that control what information a particular user can view and update. Access is determined by e-Authentication, FDW user ID and organizations as well as system administrators/sponsors of the ACMS system. Access is further restricted by authorization based on specific organizational identifiers.

23.1. Are procedures in place to detect or deter browsing or unauthorized user access?

☒ Yes
☐ No

Before a user can access the ACMS, they must obtain a level 2 e-Authentication user ID, a FDW user ID that has been assigned access to organizations and then be authorized by ACMS application administrators upon submitting a user profile. The ACMS application administrators then identify very specific access privileges and authority. Each user is restricted to specific actions and web screens by the ACMS system based on assigned roles within ACMS. Access to specific records is restricted to the organizations assigned to the FDW user ID for the ACMS user.

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

☒ Yes
□ No

To enter the ACMS website, users must have a valid FDW user ID. Users also encounter a warning notification to unauthorized use at the application website and must have registered for a level 2 e-Authentication user ID. This means, if a user tries to access ACMS and they have not previously registered for the proper e-Authentication access with the USDA CIO Security Office, they will be denied access.

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

Privacy and accessibility rules are identified and specified by the Agency ACMS system owners. System developers incorporate the appropriate security controls and the ACMS system manager maintains the specified controls. Everyone involved with ACMS is responsible for protecting the privacy rights of individuals covered in this system. Users are restricted to only view the data needed to do their jobs. System users take security training,are certified, and only have access to minimal data. ACMS is managed by the Marketing and Regulatory Programs Business Services (MRPBS), Financial Management Division (FMD).

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?
Individuals needing information pertaining to privacy rights may: (A) contact the USDA APHIS Freedom of Information and Privacy Act Staff, 4700 River Road, Unit 50, Riverdale, Maryland 20737; (B) visit the APHIS Privacy Policy site at web address: http://www.aphis.usda.gov/footer_items/index.shtml; or (C) visit the USDA Freedom of Information Act (FOIA) website at http://www.usda.gov/da/foia.htm

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

☒ Yes. If YES, go to question 28
□ No

Earlier in 2007, the Office of the USDA Secretary created a Task Force lead by the OCFO, OCIO, and the Departmental Administration to insure protection of PII. In a conversation with the APHIS FOIA and Privacy Act staff, the USDA Privacy Officer indicated that the Task Force will develop a USDA breach notification policy as well. They advised that this item could be checked off "Yes."

27.1. If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

□ Yes
☒ No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?
The system is based on agency business processes and makes no personal determinations. The system is not suited to monitor individuals or infringe on the privacy of individuals. System users are USDA employees who have undergone background investigations. System users are providing analytical or reconciliatory services for reporting purposes and data in most cases has already been processed. Furthermore, the system does not request information based on character traits (i.e. gender, race, birthday, etc).

Any user who can participate in a government program, according to the laws governing the program, receives the same equitable treatment of processed information and information for all users is processed under the same automated business rules.

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

□ Yes
☒ No. If NO, go to question 31

30.1. Explain

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
☐ No. If NO, go to question 32

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

Data can be retrieved by the following data elements:

- *First Name*
- *Middle Name*
- *Last Name*
- *Social Security Number*
- *Employee Type*
- *Location*
- *Job Title*
- *Pay Plan*
- *Grade/Step*
- *Locality*
- *Benefits Plan*
- *Appointment Type*
- *Work Schedule*
- *Hours per Pay Period*
- *Allowances*
- *Estimates per pay period provided: Salary, Benefits, Overtime, Other Pay*

The most frequent elements used for retrieval are as follows:

- *Estimates per pay period provided: Salary, Benefits, Overtime, Other Pay*
- *Last Name*
- *Social Security Number*

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

The system currently operates under the SOR Notice for EMRS which was published on April 30, 2008 under Docket No. APHIS-2008-0039. The document number is FR. Doc. E8-9418 Filed 4-29-08 8:45 a.m. The URL for accessing the SORN is: http://edocket.access.gpo.gov/2008/pdf/E8-9418.pdf

31.3. If the system is being modified, will the SOR require amendment or revision?

NO, The system is currently in operation and will operate on the notice of the EMRS.

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

☐ Yes
☒ No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect customer privacy?

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Animal and Plant Health Inspection Service (APHIS) Cost Management System (ACMS)
(System Name)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

8/7/09

System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

Tonya G. Woods

8/3/09

Agency's Chief Privacy Officer
OR Senior Official for Privacy
OR Designated privacy person

Date

Marilyn L. Holland

8/4/09

Agency OCIO

Date

8/3/09

Agency ISSP

Date