Privacy Impact Assessment

Accountability Information Management Systems (AIMS)

Revision: 1.0

Natural Resources Conservation Service

Date: June 26 2007

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

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: **USDA NRCS**

System Name: **Accountability Information Management Systems (AIMS)**

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

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

Description of the System:

Natural Resources Conservation Service (NRCS) has developed and implemented the Accountability Information Management System (AIMS) at the OCIO ITS Hosting Operations Branch (Web Farm) facility at Fort Collins, CO to enable the agency to meet each initiative within the President's Management Agenda. The AIMS is a system of data collection tools, processes, and related applications that provides conservation information in a timely manner to support the agency's strategic and performance planning and monitoring, budget formulation, business planning, operations management, workforce planning, and accountability activities. The AIMS is designed to collect high quality conservation information with minimal burden on the field, to ensure consistency nationwide in the data collected, and to make the information accessible to those who need it in a timely manner.

Who owns this system? Wendall R. Oaks, IT Application Development Branch Chief, USDA-NRCS, wendall.oaks@ftc.usda.gov, 970-492-5479.

Who is the security contact for this system? Chuck Hart, Information System Security Manager, USDA NRCS, Chuck.Hart@ftc.usda.gov, (970) 295-5550.

Who completed this document? Sandy Williams, Sr. Systems Security Analyst/CISSM, sandy.williams@ftc.usda.gov, 970-295-5558.

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**	**NO**
Social Security Number	**NO**	**NO**
Telephone Number	**YES**	**NO**
Email address	**YES**	**NO**
Street address	**YES**	**NO**
Financial data	**NO**	**NO**
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]	**YES**	**NO**
Are social security numbers embedded in any field?	**NO**	**NO**
Is any portion of a social security numbers used?	**NO**	**NO**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**NO**	**NO**

If all of the answers in Questions 1 and 2 are NO, STOP
You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:
3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[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.

Data to be used in the AIMS application is general information that can identify the customer, provide means for contacting the customer, and basic demographic information for monitoring completeness of coverage in the delivery of agency conservation programs.

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

5. Sources of the data in the system.

5.1. What data is being collected from the customer?

General information that can identify the customer, provide means for contacting the customer, and basic demographic information for monitoring completeness of coverage in the delivery of agency conservation programs.

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

NRCS, Rural Development (RD), and Farm Service Agency (FSA).

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

Conservation Districts, local and state government, and state conservation agencies.

5.4. From what other third party sources is data being collected?

None

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

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

Data created by USDA staff about outside sources is reviewed for accuracy against existing agency data, and by the employees at local offices who have knowledge of the data. The AIMS application does not have permissions for non-USDA staff data input. Completeness is checked through manual review, comparison with existing agency data, and by employees at local offices who have knowledge and responsibility of the data.

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

Data created by USDA staff about outside sources is reviewed for accuracy against existing agency data, and by the employees at local offices who have knowledge of the data. The AIMS application does not have permissions for non-USDA staff data input.

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

Completeness is checked through manual review, comparison with existing agency data, and by employees at local offices who have knowledge and responsibility of the data.

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 data is used for summary reporting and analysis. Sensitive information is not used in summary reporting. AIMS Reports are protected through the application roles and eAuthentication security.

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?

The data is used for summary reporting and analysis. Sensitive information is not used in summary reporting. AIMS Reports are protected through the application roles and eAuthenication security.

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?

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?

Stewardship through application roles and eAuthenication security of the data continues regardless of the distribution or aggregation.

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?

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?

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

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

☐ Yes
☒ No. If NO, go to question 20

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

Notice of Privacy Act System of Records by Owner, Operator or Producer Files (or Volunteer / Employee Files) USDA/NRCS-1 http://www.nrcs.usda.gov/about/foia/408_45.html.

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 managers, developers, agency field personnel, and NRCS managers.

22. How will user access to the data be determined?

Users do not have direct access to the system. All access is role-based through applications that control what information a particular user can view and update. Application access is described in the various business rules documentation that exists in the appropriate CoLab AIMS application projects.

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

☒ Yes
□ No

23. How will user access to the data be restricted?

The AIMS application system owner identifies very specific access privileges and authority. Each user is restricted to specific actions by the applications and to specific web screens by the eAuthentication (eAuth) security system. Developers only have access to the systems they are working on. Database administrators control and grant permissions for access to specific databases as authorized by the business application owners.

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

☒ Yes
□ No

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

☒ Yes
□ No

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 AIMS system owner. System developers design in the appropriate security controls and the IT General Support Systems (GSS's) manages, controls, and maintains the specified controls.

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

Customers and employees can contact the NRCS Security Response/Access Control Team via the NRCS 800 number and/or e-mail address. Additionally, each state has an Information System Security Point of Contact (ISSPOC) and a State Administrative Officer (SAO) that can be contacted at their Center or State Office.

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

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?

All NRCS systems/applications are versioned controlled through NRCS and will inherit the security controls of the hosting system/network infrastructure(s).

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.)?

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)

Notice of Privacy Act System of Records by Owner, Operator or Producer Files (or Volunteer / Employee Files) USDA/NRCS-1
http://www.nrcs.usda.gov/about/foia/408_45.html.

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

N/A

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?

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Accountability Information Management Systems (AIMS)

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.

5-16-08

Wendall R. Oaks
System Owner
Date

4-29-08

Mary Alston
NRCS FOIA/PA Officer
Date

Wendall R Oaks
5-16-08

Jack Carlson
NRCS CIO
Date