USDA

United States
Department of
Agriculture

Farm Service Agency
DAFP/CEPD
6501 Beacon Drive
Kansas City, MO 64133-4676

Date: September 4, 2008

FSA
FARM SERVICE AGENCY

Privacy Impact Assessment (PIA)

The Conservation System (CS)

- Conservation Reserve Program (CRP)
  - Conservation On-line System (COLS)
    - CRP Re-enrollment and Extensions (REX)
    - General Signup Offer Process (GSOP)
    - Continuous Sign-up Offer Process (CSOP)
    - State Areas for Wildlife Enhancement (SAFE)
    - Signup Configuration
  - Soils Database Management System (SDMS)
  - CRP Contracts
  - Conservation Legacy Upload
  - Emergency Forestry Conservation Reserve Program (EFCRP)
- Emergency Conservation Program (ECP)
- Conservation Reporting & Evaluation System (CRES)
- Grassland Reserve Program (GRP)
- CORVID (COTS)

Revision: Final V.2
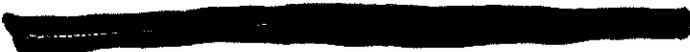
Document Information

Owner Details	
Name	Charles Michael Boyles - Manager, Price Support & Commodity Applications Office (PSCAO)
Contact Number	(816) 926-1905
E-mail Address	mike.boyles@kcc.usda.gov

Document Revision and History			
Revision	Date	Author	Comments
Draft V.1	June 26, 2008	R. Houston, EDS	Initial document
Draft V.2	July 1, 2008	Gloria Scoby PSCAO,CSSG	Updated 2.7, 3.1, 3.1.1 (1, 3,), 3.1.2 (5, 6), 3.1.4 (1, 2), 3.1.5 (4), 3.1.6 (4, 6), 3.1.7 (1.1, 1.3), 4.
Draft V.3	July 17, 2008	R. Houston, EDS	Removed edit comments, updated data use information after clarification with author. Updated contact info.
Draft V.4	August 4, 2008	R. Grant-Smith, ECS	Per Gloria Scoby, I made changes to sections 2.2.1.5 and 2.2.2.
Draft Final	August 6, 2008	R. Grant-Smith, ECS	Made changes throughout document based on recommendation from Gloria Scoby.
Final V.1	08/29/2008	R. Grant-Smith, ECS	Per Sue Busselis' recommendation, made changes to section 2.5.
Final V.2	9/4/2008	R. Grant-Smith, ECS	Per S. Nuessle's recommendation, made changes to the signature page swapping Karen Malkin, CPO, with Brian Davies, ISSPM.

Distribution List			
Name	Title	Agency/Office	Contact Information

Table of Contents

1 Purpose of Document

USDA DM 3515-002 states: "Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in USDA.

Both the system owners and system developers must work together to complete the PIA. System owners must address what data are used, how the data are used, and who will use the data. System owners also need to address the privacy implications that result from the use of new technologies (e.g., caller identification). The system developers must address whether the implementation of the owner's requirements presents any threats to privacy."

The Privacy Impact Assessment (PIA) document contains information on how The Conservation System (CS) affects the privacy of its users and the information stored within. This assessment is in accordance with NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems.*

2 Applicability

2.1 Applicability of System

The information in this document is applicable to The Conservation System (CS).

2.2 System Overview

The Conservation System major application consists of five minor applications that support the USDA Farm Service Agency mission. The minor applications consist of the Conservation Reserve Program (CRP), Emergency Conservation Program (ECP), Conservation Reporting & Evaluating System (CRES), Grassland Reserve Program (GRP), and CORVID, a commercial-off-the-shelf (COTS) program. Additionally, there are five (5) components and five (5) sub-component applications within the CRP application; these are listed below. The applications are used by USDA employees to deliver services to farmers involving environmental quality, conservation of natural resources, emergency conservation, and land use and rural development.

The system contains Personally Identifiable Information (PII) about farmers that is available to approximately 3200 USDA employees throughout the United States and US territories. No access to the system is available to the general public. Users are generally categorized by their location, having access to resources that is restricted by either the county, state, or national role that they occupy. While most users are employees of FSA, one application grants limited access to employees of NCRS to update soils information.

2.3 System Categorization

By following the guidance set forth in NIST SP 800-60 and FIPS PUB 199 taking into account the information types and other factors for this system, the Security Categorization for this system has been determined to be **Moderate**. Therefore, Risk Assessments and Security Testing and Evaluation (ST&E) will be performed following the Moderate baseline set forth in NIST SP 800-53 Annex 2.

2.4 Responsible Organization

United States Department of Agriculture (USDA)
Farm Service Agency (FSA)
1400 Independence Avenue SW
Washington, D.C. 20250

This system is maintained by:

Farm Service Agency
FSA/DAM/ITSD/ADC/PSCAO
6501 Beacon Drive
Kansas City, MO 64133

This system's hardware is located at:

- Mainframe
  IBM Z/800
  OCIO/NITC
  8930 Ward Parkway

Kansas City, MO 64110

- RS/6000 Intel-based servers
  OCIO/ITS/IOD/HOB
  8930 Ward Parkway
  Kansas City, MO 64110

- Intel-based web servers
  OCIO/ITS/IOD/HOB
  8930 Ward Parkway
  Kansas City, MO 64110

- IBM AS/400 County Office platform and workstations - nationwide

2.5 Information Contacts

Name	Title	Address	Phone Number	E-mail Address
Certifying Officer: Sue Bussells	FSA Chief Information Officer (Acting) Director, Information Technology Services Division (ITSD) (Acting) FSA/DAM/ITSD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	(202) 720-5320	sue.bussells@wdc.usda.gov
Business Owner (DAA): Robert Stephenson	Director, Conservation and Environmental Programs Division USDA/FSA/DAFP/CEPD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	202-720-6221	robert.stephenson@wdc.usda.gov
Information Owner: Charles "Michael" Boyles	Manager, Price Support & Commodity Applications Office (PSCAO) FSA/DAM/ITSD/ADC/PSCAO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-1905	mike.boyles@kcc.usda.gov
Information System Owner: Eric Will	Branch Chief, Conservation Special Systems Group (CSSG) FSA/DAM/ITSD/ADC/PSCAO/CSSG	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-2664	eric.will@kc.usda.gov
User Representative: Martin Lowenfish	DAFP/CEPD/CAB	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	202-720-3265	martin.lowenfish@wdc.usda.gov

2.6 Assignment of Security Responsibility

Name	Title	Address	Phone Number	E-mail Address
Privacy Act Officer: Karen Malkin, ESQ	Chief Privacy Act Officer USDA/FSA/OA	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-2203	karen.malkin@wdc.usda.gov
Freedom of Information Act (FOIA) Coordinator: Thomas B. Hofeller, Acting	Associate Administrator for Operations and Management USDA/FSA/OA	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-0153	tom.hofeller@wdc.usda.gov
Information System Security Program Manager (ISSPM): Brian Davies	Information Security Office (ISO) USDA/FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-720-2419	brian.davies@wdc.usda.gov
Disaster Recovery Coordinator: Mindy Gehrt	Information Security Office (ISO) USDA/FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3522	mindy.gehrt@kcc.usda.gov
Certification & Accreditation Coordinator: Georgia "Shelly" Nuessle	Information Security Office (ISO) USDA/FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3018	georgia.nuessle@kcc.usda.gov

3 USDA Privacy Impact Assessment

3.1 Does the System Contain Information About Individuals in an Identifiable Form?

QUESTION 1 Does the system contain any of the following type of data as it relates to individuals:	Yes		No
	Citizens	Employees	
Name	☒	☐	☐
Social Security Number	☒	☐	☐
Telephone Number	☐	☐	☒
Email address	☐	☐	☒
Street address	☒	☐	☐
Financial data	☒	☐	☐
Health data	☐	☐	☒
Biometric data	☐	☐	☒
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?	☒	☐	☐
Is any portion of a social security numbers used?	☒	☐	☐
Are social security numbers extracted from any other source (e.g. system, paper, etc.)?	☒	☐	☐

If all of the answers in Questions 1 and 2 are NO, 🛑

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,

---

[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.

Date: September 4, 2008

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.

3.1.1 Data Collection

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

   - **Customer:** Structure of business ventures and conservation program information is collected.
   - **Other:** Location of land is the data collected.

2. 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

3. Sources of the data in the system.

   3.1. What data is being collected from the customer?

   Conservation program information is collected form the customer.

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

   The FSA and NRCS provide practice information, business structure, and payment limitations.

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

   None.

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

   Third party sources include technical service providers and farm management consultants.

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

   ☒ Yes
   ☐ No. If NO, go to section 3.1.2, question 1.

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

   Internal validation checks are used to verify data for accuracy, relevance, timeliness, and completeness.

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

   Data is handled through NRCS (TSP).

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

Internal validation checks are used to verify data for accuracy, relevance, timeliness, and completeness.

3.1.2 Data Use

1   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 as a filtering key internally.

2   Will the data be used for any other purpose?

☐ Yes
☒ No. If NO, go to question 3 (below).

2.1   What are the other purposes?

3   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

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

☒ Yes
☐ No. If NO, go to question 5 (below).

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

☒ Yes
☐ No

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

☒ Yes
☐ No

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

Field spot checks (10% annually) are performed.

5   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?

Conservation Program Information is the intended use of all data being collected.

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

☐ Yes
☒ No. If NO, go to question 7 (below).

6.1   What are the other uses?

7   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 8 (below).

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

8   Are processes being consolidated?

☐ Yes
☒ No. If NO, go to section 3.1.3, question 1.

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

3.1.3   Data Retention

1   Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 2 (below).

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

All data in the system is maintained indefinitely.

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

N/A

1.3   Where are these procedures documented?

N/A

2   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?

Nightly backups and archives are performed. Closed/expired contracts cannot be altered. Audit trails are maintained.

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

☒ Yes
☐ No

3.1.4   Data Sharing

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

☐ Yes
☒ No. If NO, go to question 2 (below).

1.1   How will the data be used by the other agency?

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

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

☐ Yes
☒ No. If NO, go to question 3 (below).

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

3   Is the system operated in more than one site?

☒ Yes
☐ No. If NO, go to section 3.1.5, question 1.

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

The centralized distribution of applications is used to ensure the consistent use of system data. Software is the same at all sites.

3.1.5 Data Access

1 Who will have access to the data in the system (e.g. users, managers, system administrators, developers, etc.)?

County, State, and National employees plus System Administrators have access to the data in the system.

2 How will user access to the data be determined?

Role-based and tiered access - County employees can see county information, State can see state data, and National spans across the entire system.

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

☒ Yes
☐ No

3 How will user access to the data be restricted?

Role-based and tiered access is used to restrict access to data.

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

☒ Yes
☐ No

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

☒ Yes
☐ No

3.1.6 Customer Protection

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

Robert Stephenson, Director, Conservation and Environmental Programs Division

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

Robert Stephenson
Director, Conservation and Environmental Programs Division
USDA/FSA/DAFP/ CEPD
U.S. Department of Agriculture
Farm Service Agency

1400 Independence Avenue SW
Washington D.C. 20250
(202) 720-6221
robert.stephenson@wdc.usda.gov

3   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 4 (below).
☐ No

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

4   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 5 (below).

4.1   Explain how this will be mitigated?

5   How will the system and its use ensure equitable treatment of customers?

Internal controls are applied consistently without respect of race, gender, nationality, or location. There are limited actionable choices.

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

☐ Yes
☒ No. If NO, go to section 3.1.7, question 1.

6.1   Explain

3.1.7   System of Record

1   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 section 3.1.8, question 1.

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

Data is retrieved via a generated identifier number.

1.2 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)

USDA/FSA-2 – Farm Records File (Automated)

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

No.

3.1.8 Technology

1 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.

1.1 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

4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Conservation System (CS)

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.

_____   _____
Charles Michael Boyles   Date
Information Owner

_____   _____
Sue E. Bussells   Date
Agency CIO (Acting)

_____   _____
Brian Davies   Date
Information System Security Program Manager (ISSPM)