United States
Department of
Agriculture

Privacy Impact Assessment (PIA)

Data Provisioning System (DPS)

Customer Order Entry System (COES)

Farm Service Agency
Aerial Photography Field Office (APFO)
2222 West 2300 South
Salt Lake City, UT 84106

Date: September 9, 2008

Revision: Final

Document Information

Owner Details	
Name	Ronald Nicholls, Director, FSA/DAFP/APFO
Contact Number	(801) 844-29[illegible]
E-mail Address	ronald.nicholls@slc.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
Document created	07/25/2008	Lori Unlhorn, APFO	New format and update
Draft V.1	August 1, 2008	R. Grant-Smith, EDS	Formatted, Revised original document.
Final	August 1, 2008	S. Timbrook, EDS	Reviewed Original Document, Marked Final, Sent out for Signatures
Corrections	August 21, 2008	Lori Unlhorn, APFO	Corrections made, Signatures
Final	09/09/2008	S. Timbrook, EDS	Signatures received
	11/06/2009	S. Timbrook, ECS	Minor revision for completeness and clarity. Section 2.8.1, 2.8.4, 2.8.5, 2.8.6.

Table of Contents

1 Purpose of Document

USDA DM 3515-002 states: "Agencies are responsible for initiating the Privacy Impact Assessment (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 (i.e., 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 **Data Provisioning System (DPS)** 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 Data Provisioning System (DPS). DPS consists of one (1) application:

- Customer Order Entry System (COES)

2.2 System Overview

The Data Provisioning System (DPS) is a web based, Commercial-off-the-Shelf (COTS) package that accesses APFO's existing geospatial data catalog. The Customer Order Entry System (COES) is a module of DPS that allows customers to access, select, and purchase imagery on-line. The validation of credit cards is managed by a third party payment service provider known as PayPal.

The DPS system resides on Sun Servers that employ a Linux OS. Data for the system resides on a Sun ES 6500 server that houses a large Oracle database. This hardware and software is encompassed within the APFO General Support System (GSS) infrastructure.

Access to the Data Provisioning System consists of internal and external users:

- Internal user access is determined via role based authentication controls. The monitoring of access logs by administrators ensures that no unauthorized personnel access data without authorization. The only user interface with the system is through the hummingbird terminal emulation program and that access is a menu driven "portal" that controls users' access. These internal users consists of FSA Aerial Photography Field Office (APFO) and State and County Office (SCO) staff that have a need to access and input/update the necessary data to effectively deliver and administer the system.
- Access by external users is managed thru Access Control Lists (ACL) and new accounts are approved by IT Manager prior to creation. Direct access to data is restricted via ACL's and configured thru server services as opposed direct access from user's accounts. When a request for data is made, the system creates "pseudo links" where the data can be downloaded. External users include other Federal (DHS, FEMA, NOAA), commercial vendors and private customers.

The COES minor application will be available to the public via the USDA public facing Internet: www.fsa.usda.gov or www.usda.gov. Public users will be able to access, select, and purchase imagery on-line. The validation of credit cards is managed by a third party payment service provider known as PayPal. Customers may also go to local FSA State and County Offices and request photographic imagery.

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
Aerial Photography Field Office (APFO)
2222 West 2300 South
Salt Lake City, UT 84106

This system's hardware is located at:

OCIO/ITS – OCIO/ITSD
FSA-Aerial Photography Field Office
2222W 2300S
Salt Lake City, UT 84119-2020

2.5 Information Contacts

Name	Title	Address	Phone Number	E-mail Address
Certifying Officer: Steve Sanders	FSA Chief Information Officer Director, Information Technology Services Division (ITSD) FSA/DAM/ITSD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	(202) 720-5320	steve.sanders@wdc.usda.gov
Business Owner (DAA): Ronald Nicholls	Director, Aerial Photography Field Office (APFO) FSA/DAFP/APFO	U.S. Department of Agriculture Farm Service Agency 2222 West 2300 South Salt Lake City, UT 84119	(801) 844-2907	ronald.nicholls@slc.usda.gov
Business Program Manager: Ronald Nicholls	Director, Aerial Photography Field Office (APFO) FSA/DAFP/APFO	U.S. Department of Agriculture Farm Service Agency 2222 West 2300 South Salt Lake City, UT 84119	(801) 844-2907	ronald.nicholls@slc.usda.gov
System Owner: Kenneth Koehler	Chief, Operations Branch Photography Field Office (APFO) FSA/DAFP/APFO	U.S. Department of Agriculture Farm Service Agency 2222 West 2300 South Salt Lake City, UT 84119	(801) 844-2903	kenneth.koehler@slc.usda.gov
System Manager: Lori Uhlhorn	Chief, Technology Services Branch Photography Field Office (APFO) FSA/DAFP/APFO	U.S. Department of Agriculture Farm Service Agency 2222 West 2300 South Salt Lake City, UT 84119	801-844-2970	lori.uhlhorn@slc.usda.gov

2.6 Assignment of Security Responsibility

Identify person(s) responsible for security of the application/system and an alternate emergency contact.

Name	Title	Address	Phone Number	E-mail Address
Application/ System Security Personnel: Brian Davies	Information System Security Program Manager (ISSPM) 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
Mindy Gehrt	Disaster Recovery Coordinator Information Security Office (ISO) 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
Georgia "Shelly" Nuessle	Certification & Accreditation Coordinator Information Security Office (ISO) 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

2.7 Who Completed this Assessment?

July 25, 2008
Lori Uhlhorn
Chief, Technology Services Branch
U.S. Department of Agriculture
Farm Service Agency
Photography Field Office (APFO)
2222 West 2300 South
Salt Lake City, UT
84119
801-844-2970
lori.uhlhorn@slc.usda.gov

USDA Privacy Impact Assessment

2.8 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 (i.e. system, paper, etc.)?	☐	☐	☒

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

[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.

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.

2.8.1 *Data Collection*

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

   The Data Provisioning System (DPS) contains a catalog of available geospatial data. The Customer Order Entry System (COES) is a web based, on line order transaction system. Validation of credit cards is managed by a third party.

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?

   The customer's shipping address and preferred payment method will be collected.

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

   None.

   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?

   Imagery data is contracted annually to multiple vendors.

4. 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 section 3.1.2, question 1.

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

   Shipping address and preferred payment method will be collected from the customer.

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

All data is entered via the agencies users. Users have manual processes in place to ensure the accuracy of the data being entered into the system.

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

The validation of credit cards is managed by a third party payment service provider known as PayPal.

2.8.2 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?

Data is being collected to ensure accurate billing for imagery purchased.

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 (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

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

The system is not designed to derive new data about a customer, but it could be performed manually.

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

☐ Yes
☒ No

The customer's shipping address and preferred payment method will be collected.

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

☐ Yes

☒ No

Extrapolation of the data or determination about the customer is made by the system.

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

Only sales employees granted the WEBREFUND role have access to the screen required to enter the data.

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?

Payment, shipment, and refunds are the intended routines.

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?

N/A

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?

N/A

8 Are processes being consolidated?

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

The data is consolidated by design. Centralized Oracle relational database instance with authentication methods are being employed. Permissions are set within the database structure to keep unauthorized queries and programs from accessing data

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

Role based group authentication controls who enters data and monitoring of access logs by administrators ensures that no unauthorized personnel access data without authorization. The only user

interface with the system is through the hummingbird terminal emulation program and that access is a menu driven "portal" that controls users' access.

2.8.3 Data Retention

1 Is the data periodically purged from the system?

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

Financial and contracting data is retained a minimum of 6 years. However, as APFO is charged with archiving of aerial imagery and its associated information, all data is archived via automated processes.

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

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

1.3 Where are these procedures documented?

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?

As customers make new purchases, existing information is verified. The imagery is "static" data.

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

☒ Yes
☐ No

2.8.4 Data Sharing

1 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 2 (below).

Accounts are created for individual users within other Federal agencies. The availability of these accounts is event driven (i.e., Disaster Response) and users must request accounts in advance. These agencies include NOAA, FEMA, DHS, and their associated contracted staff.

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

APFO's geospatial data is used for emergency planning, disaster response, census, agriculture, and event security.

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

Geospatial data produced by APFO is in the Public Domain. APFO assures this process thru roles and Access Control Lists (ACL) where requestors are restricted to read only.

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?

Yes

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?

2.8.5 Data Access

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

All APFO Personnel, Developers, DBA's, SAs, external Federal, Commercial and Private Customers

2 How will user access to the data be determined?

Access is determined by the user's position within APFO and controlled via role-based authentication.

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

☒ Yes
☐ No

3 How will user access to the data be restricted?

Access is determined by the user's position within APFO and controlled via role-based authentication. This access is documented within the administrator's manual. Access by external customers is managed thru ACL's and new accounts are approved by IT Manager prior to creation. Direct Access to data is restricted via ACL's and configured thru server services as opposed direct access from user's accounts. When a request for data is made, the system creates "pseudo links" where the data can be downloaded.

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

☒ Yes

☐ No

Role based group authentication controls who enters data and monitoring of access logs by administrators ensures that no unauthorized personnel access data without authorization. The only user interface with the system is through the hummingbird terminal emulation program and that access is a menu driven "portal" that controls users' access.

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

☐ Yes
☒ No

2.8.6 Customer Protection

1 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.)?

Ronald Nicholls, Director APFO (DAA)

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

Customers can contact the USDA/FSA Privacy Officer at the following address:

Name	Address	Phone Number	E-mail Address
Chief Privacy Act Officer: Karen Malkin , ESQ	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 2025	202-690-2203	karen.malkin@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?

N/A

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

FSA guidelines for fair and equitable treatment already exist.

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

2.8.7 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 (i.e. employee number, social security number, etc.)?

Primary access to the system is through the Exceed Corporation's Hummingbird terminal emulation program, which allows a menu driven application interface. The menu was developed using the following Oracle applications, SQL Report Writer, and SQL Forms, as the front-end interface with the Oracle RDBMS. PDS system is controlled, administered, and maintained by APFO.

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)

- Subsidiary Personnel, Pay and Travel Records, USDA/FSA-11
- Applicant/Borrower, USDA/FSA-14
- GOVT-1: General Personnel Records (TXT 32KB)

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

No.

2.8.8 Technology

1 Is the system using technologies in ways not previously employed by the agency (i.e. 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

USDA FSA Privacy Impact Assessment for Data Provisioning System (DPS)

3 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Data Provisioning System (DPS)

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.

Ronald B. Nicholls — 13-Aug-08

Ronald Nicholls — Date

System Owner

Steven L. Sanders — Date

Agency CIO

Karen Malkin — Date

Associate Administrator for Operations and Management

Acting Senior Official for Privacy

USDA FSA Privacy Impact Assessment for Data Provisioning System (DPS)

3 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Data Provisioning System (DPS)

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.

Kenneth Koehler Date

System Owner

Sue E. Bussells 9/2/08

Sue Bussells Date

Agency (Acting) CIO

Karen Malkin Date

Associate Administrator for Operations and Management

Acting Senior Official for Privacy

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Data Provisioning System (DPS)

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.

Kenneth Koehler
System Owner

Date

Sue Bussells
Agency (Acting) CIO

Date

Brian Davis

9/9/2008

Brian Davies
Information System Security Program Manager (ISSPM)

Date