USDA

Privacy Impact Assessment (PIA)

Processed Commodities Inventory Management System
PCIMS

Revision: Final

Farm Service Agency

FSA
FARM SERVICE AGENCY

Date: May 10, 2010

Document Information

Business Owner Details	
Name	Rosemary Hall
Contact Number	(816)926-1975
E-mail Address	Rosemary.Hall@kcc.usda.gov

Document Revision and History			
Revision	Date	Author	Comments
1.00	03/30/20 10	T. Ostrander	Removed System of Record from page 14 top row left column of table.
1.01	03/31/2010	T. Ostrander	Populated document.
1.02	04/13/2010	K. Winburn	Update and Review document
1.03	4/26/20 10	T. Ostrander	Made changes per C. Niffen from John Underwood.

Table of Contents

1 Purpose of Document

USDA DM 35 15-002 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 Processed Commodities Inventory Management System (PCIMS) 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 System Information

	System Information
e	
odities Inventory Management System (PCIM	
at	
ort Syst	
pplicat	
odities Inventory Management System (PCIMS) is anagement System (IDMS) that was developed to as eting Service (AMS), Farm Service Agency (FSA) a n Service (FNS) in the commodity purchase a rams to provide food to recipients ldwide. FSA cquisition, management, storage, disposition sportation, and accounting activities; PCIMS suppo r processed commodit	
enCSO	
64	
kcc.usda.	
m Security Program Manager (IS SP of Agricult e ce Avenue . 20 c us/ov	
ncy, C	
64	
kcc.usda.	

3 Data Information

3.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Customer: Company (not individual) tax ID number, name, and address information from the Warehousemen, Vendors, and Processors. Employee: Marketing Specialist names and work contact data.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	Yes No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.
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.	Ye s No
4	Sources of the data in the system.	Customer: Processed Commodity Storage Agreement, Contract documents completed by the various customers. Employee: manually entered into table entries PCIMS maintains information in its own database. Long Term Contracting System (LTCS) Domestic Electronic Bid Entry System (DEBES) Commodity Operation Systems (COS) Electronic Commodity Ordering System (ECOS) Minneapolis Federal Reserve Bank (MNFRB) Electronic Distribution of Disbursement Data (ED3)

No.	Question	Response
4.1	What data is being collected from the customer?	Company (not individual) tax ID number, name, and address information from the Warehousemen, Vendors, and Processors.
4.2	What USDA agencies are providing data for use in the system?	USDA/FSA, USDA/FNS, USDA/AMS
4.3	What state and local agencies are providing data for use in the system?	FNS state offices
4.4	From what other third party sources is data being collected?	None
5	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 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Data validation routines are in place when data is accepted into the system.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data validation routines are in place when data is accepted into the system.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data validation routines are in place when data is accepted into the system.

3.2 Data Use

No.	Question	Response
6	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?	To support the annual acquisition, contract awards, storage payments, invoicing, shipments, tracking, and distribution of commodities acquired by USDA for domestic and foreign food assistance programs and market support purposes.
7	Will the data be used for any other purpose?	Yes No – If NO, go to question 8.
7.1	What are the other purposes?	

No.	Question	Response
8	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	Ye s No
9	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 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	Ye s
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	Ye s No
9.3	How will the new data be verified for relevance and accuracy?	
10	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?	To support the annual acquisition, contract awards, storage payments, invoicing, shipments, tracking, and distribution of commodities acquired by USDA for domestic and foreign food assistance programs and support purposes.
11	Will the data be used for any other uses (routine or otherwise)?	Yes No – If NO, go to question 12.
11.1	What are the other uses?	
12	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 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	User's access is restricted by role-based internal access security controls within the application and by ACF2

No.	Question	Response
13	Are processes 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?	User's access is restricted by role-based internal access security controls within the application and by ACF2

3.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	Yes No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	
14.2	What are the procedures for purging the data at the end of the retention period?	
14.3	Where are these procedures documented?	
15	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?	Program data is reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and when any required updates are made.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	Ye s No

3.4 Data Sharing

No.	Question	Response
17	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 18.
17.1	How will the data be used by the other agency?	Acceptable use requirements and further disclosure restrictions are identified in the applicable Memorandum of Understandings (MOUs) and Interconnection Security Agreements (ISAs).
17.2	Who is responsible for assuring the other agency properly uses the data?	System owners and all authorized personnel with access to the application.

No.	Question	Response
18	Is the data transmitted to another agency or an independent site?	Yes No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	Yes, MOU's and ISA's are in place.
19	Is the system operated in more than one site?	Yes No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	

3.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	Production update: Customers, internal users, System Administrators. Production inquiry: Developers. Test update/inquiry: Internal users, System Administrators, and developers.
21	How will user access to the data be determined?	User's access is restricted by role-based internal access security controls within the application.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	Yes No
22	How will user access to the data be restricted?	Access is restricted through screens based on user ID.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	Yes
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	Yes No

3.6 Customer Protection

No.	Question	Response
24	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.)?	System owners and all authorized personnel with access to the application
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	FSA National Help Desk at (800)-255-2434 or the Centralized Help Desk at 800-457-3642 or By contacting John W. Underwood, Privacy Officer, at FSA Privacy Act Officer / FSA PII Officer USDA - Farm Service Agency Beacon Facility - Mail Stop 8388 9240 Troost Avenue Kansas City, Missouri 64131-3055 Phone: 816-926-6992 Cell: 816-564-8950 Fax: 816-448-5833 mailto:john.underwood@kcc.usda.gov
26	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 27. No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	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 28.
27.1	Explain how this will be mitigated?	

No.	Question	Response
28	How will the system and its use ensure equitable treatment of customers?	By providing a standardized method of performing annual acquisition, contract awards, storage payments, invoicing, shipments, tracking, and distribution of commodities activities.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	Yes No – If NO, go to question 30
29.1	Explain	

No.	Question	Response
30	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 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	OLQ's, WebFOCUS inquires, Batch Processing. Various reports may be accessed by authorized users.
30.2	Under which Systems of Record (SOR) notice 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) USDA/FSA-14 Applicant/Borrower.
30.3	If the system is being modified, will the SOR require amendment or revision?	Yes

4 Technology

No.	Question	Response
31	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.

No.	Question	Response
31.1	How does the use of this technology affect customer privacy?	

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-1 1, 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 FOR CYBER SECURITY.

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

   Processed Commodities Inventory Management System (PCIMS)
(System Name)

This document has been completed in accordance with the requirements of the E-Government 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.

_____   _____
Rosemary Hall, Information System Owner   Date

_____   _____
John Underwood, Chief Privacy Officer   Date

_____   _____
James Gwinn, FSA CIO   Date

Privnc!f Imps c L s es orrant Authalration Uumorandum

I have carefully assessed the Privacy Impact Assessment for the

Processed Commodities Inventory Management System (PCIMS) _____
(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to

authorized.

_____ 04/13/10

Rosemary Hall, Information System Owner   Date

_____ 4/21/10

John Underwood, Chief Privacy Officer   Date

_____ 4/2-Y72-t)r

James G72(, FSA CIO   Date

proceed. Based on our authority and judgment, the continued operation of this system is