Privacy Impact Assessment (PIA)

Payment Systems (Payment)
Financial Services System (FSAFS)

Revision: Final

Farm Service Agency

Date: March 23, 2010

Document Information

Owner Details	
Name	Jim McAfee, Chief PMO
Contact Number	(816) 926-6022
E-mail Address	Jim.McAfee@kcc.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
	07/11/2008	Matthew Tellado	
Draft V.1	12/02/2008	S. Timbrook, ECS	Updated original document to new 2009 template.
1.02	7/20/2009	D.Brizendine	Review with template update
1.03	7/22/09	D.Brizendine	Added revision to Questions 24, 25, 26
1.04	7/28/09	Matthew Tellado	Update by application point of contact
1.05	7/31/09	D.Brizendine	Document review; template update
1.06	8/6/2009	D.Brizendine	Updated responses for 30.2 and 30.3
1.07	8/20/2009	D.Brizendine ISO	Updated responses for 2.1, 28 and 29.1 from John Underwood email.
1.08	8/27/09	D.Brizendine ISO	After follow up with Matthew Tellado, we can answer 4.4 - "NO" – and the response to question 5.3 is "N/A".
Final	9/25/09	D.Brizendine FSAISO	Added completed Approval page and marked document as Final.
1.09	03/05/3010	S. Timbrook, ECS	Review and update from baseline 2010
	03/17/2010	S. Timbrook, ECS	Uploaded to SharePoint for final review and released for signatures.
	03/23/2010	S. Timbrook, ECS	Released for final signatures.
	04/13/2010	S. Timbrook, ECS	Updated with J Underwood comments 30.2
	04/14/2010	S. Timbrook, ECS	Changed business owner to Jim McAfee from Brent Reinhardt.

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 **Payment System (Payment)- Financial Services System (FSAFS)** 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	
Agency:	Farm Service Agency
System Name:	Payment System (Payment)- Financial Services System (FSAFS)
System Type:	Major Application General Support System Non-major Application
System Categorization (per FIPS 199):	High Moderate Low
Description of System:	FSA Financial Services is an application that will enable customers and service center employees to enter and maintain direct deposit, assignment and joint payment information for FSA customers. Financial Services is the source of customer/vendor information used by NPS/Online Payments to make payments and by NRRS to create debts. FSA Financial Services will perform the following functions: • Validate information entered for single year or multi year assignments. • Validate direct deposit banking information entered for producers and facilities. • Validate joint payment information entered for producers and facilities.
Who owns this system? (Name, agency, contact information) Information Owner.	Brent Reinhardt Group Chief, Service Center Accounting and Debt Group U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133 (816) 926-6438 Brent.Reinhardt@kcc.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information System Security Program Manager (IS SPM) U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250 (202) 720-2419 brian.davies@wdc.usda.gov

Who completed this document? (Name, agency, contact information)	Shahara Timbrook, ECS 1500 E. Bannister Road Kansas City, MO 64131 (816) 823-5823	

3 Data Information

3.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Profile of User including Name, address, banking information
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, SCIMS
4.1	What data is being collected from the customer?	Banking and financial information is collected from the customer directly. Other data is collected by other source systems.
4.2	What USDA agencies are providing data for use in the system?	Farm Service Agency
4.3	What state and local agencies are providing data for use in the system?	None
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.

No.	Question	Response
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Banking information is checked to verify accuracy of bank via routing number, Assignments require approval of assignee.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data from USDA sources are checked for accuracy and completeness upon entry into the source system. The source system will initiate a real time request to update the altered data in Financial Services. Since Financial services does not own the data received by other systems, it does not alter the data but only updates it when the source system tells it
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A

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 allow the customers to be paid either by check or direct deposit through National Payments System (NPS) and receive 1099's, notices of changes of banking, and transaction statements.
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?	N/A
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	Yes 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)?	Yes
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	Yes No

Date: April 16, 2010

No.	Question	Response
9.3	How will the new data be verified for relevance and accuracy?	N/A
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 allow the customers to be paid either by check or direct deposit through National Payments System (NPS) and receive 1099's, notices of changes of banking, and transaction statements.
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?	N/A
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?	Level 2 E-auth is required for access to system.
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?	N/A

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?	N/A
14.2	What are the procedures for purging the data at the end of the retention period?	N/A
14.3	Where are these procedures documented?	N/A

No.	Question	Response
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?	Source system of personal data updates us of changes. Financial Data is able to be updated by customer.
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?	N/A
17.2	Who is responsible for assuring the other agency properly uses the data?	N/A
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?	N/A
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?	N/A

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.)?	Users, system administrators, business analysts, developers.
21	How will user access to the data be determined?	Access must be requested through FSA- 1 3A security forms with justification.

No.	Question	Response
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	Ye s No
22	How will user access to the data be restricted?	Users are restricted through role-based security within the application. Other users are restricted by based on id level security granted through eAuth/EAS and database administrators.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	Ye s
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	Ye s 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.)?	USDA Privacy Office
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	By contacting John Underwood, Privacy Officer, at john.underwood@kcc.usda.gov & 816.926.6992
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.	N/A

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?	N/A

No.	Question	Response
28	How will the system and its use ensure equitable treatment of customers?	By providing a centralized and standardized method of making payment transactions.
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	N/A

4 System of Record

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.)?	Social Security Number, and Tax Id Type
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-13, Claims Data Base: National Receipts and Receivables System (NRRS) (Automated), USDA/FSA- 14, Applicant/Borrower
30.3	If the system is being modified, will the SOR require amendment or revision?	Ye s

5 Technology

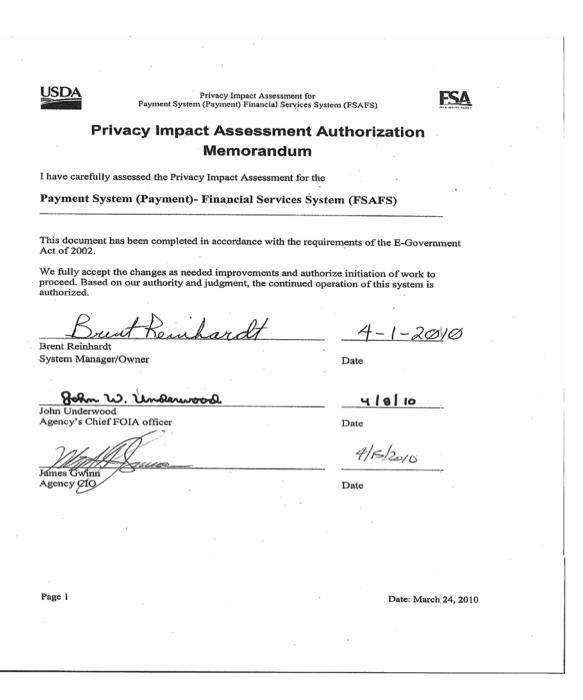| No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	Yes No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	N/A

6 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

Payment System (Payment)- Financial Services System (FSAFS)

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.

Brent Reinhardt   _4-1-2010_

Brent Reinhardt
System Manager/Owner   Date

John W. Underwood   _4/8/10_

John Underwood
Agency's Chief FOIA officer   Date

     _4/15/2010_

James Gwinn
Agency CIO   Date

Page 1   Date: March 24, 2010