Privacy Impact Assessment (PIA)
General Sales Manager Data Mart (GSMDM)

Revision: Final

Farm Service Agency

Date: June 17, 2010

Document Information

Business Owner Details	
Name	Agnes Leung, FSA/OBF/FMD/ITOC Mark Rowse, FAS/OTP/CP
Contact Number	Agnes Leung (703) 305-1426 Mark Rowse (202) 720-0624
E-mail Address	Agnes.Leung@wdc.usda.gov Mark.rowse@usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.01	May 11, 2010	Anita Trader, ISO DR	Initial version for 2010 copied from 2009 PIA.
	June 17, 2010	S. Timbrook, ECS	Reviewed, updated system description released for signatures.
	August 19,2010	C. Niffen	Changed per John Underwood questions 15, 30.2
Final	8/24/2010	R. Barbee, ECS	Finalized document by adding signature page.

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 **General Sales Manager Data Mart** 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:	General Sales Manager Data Mart.
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	The General Sales Manager Data Mart (GSMDM) supports the FSA/FAS General Sales Manager Export Credit Guarantee System (GSM) which provides the accounting system for the Commodity Credit Corporation (CCC) Export Credit Guarantee programs. The purpose of the GSMDM system is to streamline the reporting process by implementing a common computing procedure that accommodates the programming team in performing maintenance of the financial data collected by the GSM Web PC application. The Data Warehouse Team and its users can create ADHOC queries and reports as needed along with canned reports to be posted to the intranet.
Who owns this system? (Name, agency, contact information)	Angela J. Sieg, Chief AFAO Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133 (816) 926-1568 angela.sieg@kcc.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information System Security Program Manager (ISSPM) 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)	Chris Caruthers, AFAO-AGG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6848 christophor.caruthers@kcc.usda.gov

3 Data Information

3.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Customer – Evidence of export, NOD, NOA, claims, fees, guarantee bank name, account number. Employees – Interest rates, bank and country limits.
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.	☒ Yes ☐ No
4	Sources of the data in the system.	Customer, banks, Treasury Department.
4.1	What data is being collected from the customer?	Customer – Evidence of export, NOD, NOA, claims, fees, guarantee bank name, account number. Employees – Interest rates, bank and country limits.
4.2	What USDA agencies are providing data for use in the system?	FAS and FSA both own portions of the database data.
4.3	What state and local agencies are providing data for use in the system?	N/A.
4.4	From what other third party sources is data being collected?	Treasury Department and State Department.
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?	Data collected from the customer is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data collected from USDA sources is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data collected from non-USDA sources is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

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 streamline the reporting process by implementing a common computing procedure that accommodates the programming team in performing maintenance of the financial data collected by the GSM Web PC application.
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 ☐ No

No.	Question	Response
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☐ No
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 streamline the reporting process by implementing a common computing procedure that accommodates the programming team in performing maintenance of the financial data collected by the GSM Web PC application.
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?	N/A.
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.

No.	Question	Response
14.3	Where are these procedures documented?	N/A
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?	Fairness in making determinations is assured when the 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?	☒ Yes ☐ 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?	Data is reported to Treasury Department, State Department, USAID, Congress, and Paris Club; however, it is shared via reports passed from the system owners rather than the other agencies having access to the system.
17.2	Who is responsible for assuring the other agency properly uses the data?	FMD/FAS management.
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?	MOU between NITC and Treasury 11/2009.
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?	Administrative controls and procedures are established to maintain consistent system use.

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.)?	WDC Users, Farm Service Agency employees, Foreign Agriculture Service employees.

No.	Question	Response
21	How will user access to the data be determined?	Access must be requested through FSA-13A security forms with justification
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ 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. Once access has been properly granted, there are no restrictions to viewing the data. Update capabilities are restricted by User ID.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No
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.)?	FSA Privacy Act Officer/FSA PII Officer.
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

No.	Question	Response
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.
28	How will the system and its use ensure equitable treatment of customers?	Implementing a common computing procedure will be accomplished in the same manner for all customers.
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.

Date: June 17, 2010

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.)?	Data is retrieved in a variety of ways – the data is not put into an individual table to easily access an identifier; however, the combination of the tables/data might give a link to identify data if the person using the data knew how to link the tables and how to relate the identifiers.
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) and USDA/FSA-14 - Applicant/Borrower
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

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-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 FOR CYBER SECURITY.

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

General Sales Manager Data Mart

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.
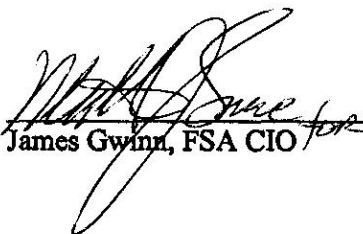
_____   8/13/10
Angela Sieg, Chief, Information System Owner   Date

_____   8/17/10
John Underwood, Chief Privacy Officer   Date

_____   8/24/2010
James Gwinn, FSA CIO   Date