USDA UNITED STATES DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

INVESTMENT: RMA Investment 07: SDA/Data Warehousing and Data Mining

RMA

September 2006

TABLE OF CONTENTS

A. GENERAL SYSTEM/APPLICATION INFORMATION

1. System Owner:

Name	Title	Phone No.	Office
Garland Westmoreland	**Director**	**202.720.5828**	**SDAA**

2. Other individuals completing this form:

Name	Title	Phone No.	Office
Kirk Bryant	**Deputy Director**	**919.875.4853**	**SDAA**
Susan Hughes	**COR/Program Analyst**	**254.918.7686**	**SDAA**

3. System/Application Name: **System** - Data Warehousing and Data Mining programs – **Application Name** - Strategic Data Acquisition and Analysis/ Data Warehousing and Data Mining

Briefly describe the purpose of this system. To use data warehousing and data mining technologies to assist RMA with identifying potential program weaknesses and insured producers, insurance agents and loss adjusters who exhibit anomalous claim outcomes that may be indicative of waste, fraud and abuse

4. Describe what agency function/mission does it support? Data warehousing and data mining directly supports RMA Strategic Plan Objective to improve program integrity and to comply with the Agricultural Risk Protection Act of 2000 requirements that FCIC/RMA use data warehousing and data mining technologies to identify producers, agents and adjusters that exhibit anomalous claim outcomes.

B. PRIVACY IMPACT ASSESSMENT (PIA) THRESHOLD

PIA’s are required to be performed and updated as necessary where a system change creates new privacy risks (for more examples, review *M-03-02, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*).

1. Is the system a new system or a system undergoing a major change?

___ ____ Yes, (Proceed to question 2)

____X___ No, (PIA not required, proceed to Appendix A) *

2. Does the system collect or maintain information in identifiable form from or about members of the public?

___X____ Yes, (PIA required, proceed to question 3)

________ No, (PIA not required, proceed to Appendix A)

3. Check below whether this Privacy Impact Assessment supports a proposed new system or a proposed modification to an existing system.

_____ _____ New System __________ Modify Existing System

*The PIA is being reassessed due to recommendations from a GAO audit. The system is not new and there are no major changes.

C. SYSTEM DATA INFORMATION

Type of information maintained in the system

1. Describe the information to be used in the system in each of the following categories (Customer, Employee, Other):

Customer (RMA staff) – producer farm level data that is reported to the Approved Insurance Providers (AIP), who in turn, transmit the data to FCIC/RMA. Agent and Adjuster data reported to the AIP is also transmitted from RMA to the Data Warehouse **Employee –** N/A. **Other –** FCIC actuarial documents, M-13 data (1990 through the present) maintained in the FCIC data acceptance system, NASS data, NOAA weather data, soils data, GIS data and RMA Compliance tracking system data.

2. What information is to be collected (e.g., nature and source)?

Farm level data that is reported by producers to the Approved Insurance Providers (AIP) to obtain crop insurance coverage. The AIPs transmits the producer, agent and adjuster data to FCIC/RMA as required by FCIC rules and FCIC/RMA transmits the data to the Center for Agribusiness Excellence (CAE) data warehouse.

3. Why is the information being collected (e.g., to determine eligibility)?

Producers, provide farm level data as a requirement for participating in the Federal Crop Insurance program. AIP’s provide the policy holder data to FCIC/RMA through data transmissions and also provide the agent and adjuster data to the Center for Agribusiness Excellence (CAE). CAE uses the data to identify anomalous data outcomes by producers, agents and adjusters.

4. What is the intended use of the information (e.g., to verify existing data)?

Data warehousing and data mining directly supports RMA Strategic Plan Objective which is to improve program integrity and to comply with the Agricultural Risk Protection Act (ARPA) of 2000. ARPA required FCIC/RMA to use data warehousing and data mining technologies to identify producers, agents and adjusters that exhibit anomalous behavior and policy outcomes and to assist FCIC/RMA in improving the integrity of the crop insurance program.

5. How will the information be shared (e.g., another agency for specified programmatic purpose)?

SDAA/CAE only provides data to approved USDA/RMA users. The Users are instructed, in writing, to obtain approval from the RMA Administrator before providing the information outside of the agency.

6 What RMA data is being collected from files and databases for this system? If yes, identify.

FCIC/RMA policyholder database (DAS), M-13 data through the Data Acceptance System, and FCIC/RMA actuarial data.

7 What Federal Agencies are providing data for use in the system?

NOAA weather data, NASS agricultural statistical data, USDA drought data.

8. What State and Local Agencies are providing data for use in the system?

None

9. From what other third party sources will data be collected?

None

10. What information will be collected from the customer/employee?

RMA staff are the customers and information about RMA employees is not transmitted to the data warehouse.

11 How will data be collected from sources other than the RMA records and the customer be verified for accuracy?

RMA is the only provider of data for the warehouse.

12. How will data be checked for completeness?

Data transmitted to the Center for Agribusiness Excellence (CAE) is subject to extensive quality control reviews to ensure the entire data set is received. CAE conducts further quality, both automated and manual, control checks before it is entered into the data warehouse and data mining programs.

13. Is the data current? How do you know?

The data in the warehouse is downloaded from FCIC on a biweekly basis. FCIC/RMA is responsible for data integrity and data transmitted to SDAA/CAE.

D. <u>ACCESS TO THE DATA</u>

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Only the CAE Database Administrators will have direct access to the policyholder and other data. The data is reformatted from the FCIC DAS data into a format compatible with the database warehouse where it is stored read-only. Developers can query the data but they will only see the results from their queries. Approved users will be able to view the results from the data but will not be allowed to make queries or view the raw data.

2. How is access to the data by a user determined?

A potential user must contact the RMA Security Liaison Representative and Contracting Officer Representative at CAE and the SLR/COR will submit an FCIC-586 user request security form to the RMA Security Staff. If the Security Staff approves the request, the user will be issued a password by SDAA/CAE.

3. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?

Yes; RMA Security and SDAA/CAE Security document the procedures in the standard operating procedures and security plan.

4. Will users have access to all data on the system or will the user’s access be restricted? Explain.

The user access is restricted. The user will have access to the data required to perform their job but will not have access to the raw data.

5. 5. What controls are or will be in place to prevent the misuse (i.e. unauthorized browsing, unauthorized use) of data by those having access?

There are controls in place for each function performed in the system and the audits of these controls are tracked by SDAA.

6. Do other systems share data or have access to data in this system? If yes, explain.

NO

7. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface?

The privacy rights are protected by the security controls and the Privacy Act implemented by the RMA Systems Administrators and documented in the RMA Security Plan.

8. Will other agencies share data or have access to data in this system (International, Federal, State, Local, and Other)? If yes, explain.

None

9. How will the data be used by the agency?

The data warehousing and data mining technologies will be used, as legislated, as tools in identifying agents, adjusters and producers that exhibit anomalous behavior and to assist FCIC/RMA in determining potential program vulnerabilities.

10. Who is responsible for assuring proper use of the data?

The proper use of the data will be determined by the “customer” of this project, in this case approved USDA and RMA staff.

E. ATTRIBUTES OF DATA

1. Is the use of the data both relevant and necessary for the purpose for which the system is being designed?

Yes

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No. Data will not be altered or otherwise generated.

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

No. However, data may be used for further review by RMA.

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

Yes. The system is designed to identify potential patterns of abuse by producers, agents and adjusters that would otherwise be difficult for an individual to research manually.

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

The data is taken from the FCIC/RMA databases that are subject to data integrity controls.

6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

N/A

8. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Data is retrieved is retrieved through a user interface that is behind the RMA VPN, firwall and password protected. The system's end users can view data that is delivered to them via a password protected user interface.

9. What are the potential effects on the due process rights of customers and employees of?

RMA and USDA staff employees should not be effected by the data warehouse and data mining activities.

10. How are the effects to be mitigated?

N/A

F. MAINTENACE OF ADMINISTRATIVE CONTROLS

1. Explain how the system and its use will ensure equitable treatment of customers and employees.

The system does not effect the privacy of the RMA and USDA staff.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A – the data mining warehouse and data mining systems are operated at the Center for Agribusiness Excellence (CAE), in Stephenville, Texas, Tarleton State University.

3. Explain any possibility of disparate treatment of individuals or groups.

The data warehousing and data mining system is designed to identify anomalous behavior and is not, in itself, an accusation of misconduct on the part of the producer, agent or adjuster. There may be reasons for the anomalous behavior that fall within the rules and regulations of the Federal Crop Insurance program.

4. What are the retention periods of data in this system?

Data is retained by the system for the life of the project and contract.

5. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

The data is the property of RMA and data will be returned to the Kansas City RMA Office at the end of the contract.

6. 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?

The data is received bi-weekly from RMA and once loaded into the CAE data warehouse, all data on the system is updated. The data received from RMA and loaded into the data warehouse is subject to extensive quality controls.

7. Is the system using technologies in ways that the USDA has not previously employed (i.e. Caller-ID)?

No. RMA has employed data mining technologies for five years at RMA and USDA has other data mining operations in use currently.

8. How does the use of this technology affect customer/employee privacy?

RMA and USDA staff are not affected due to privacy information of employees is not maintained or acquired by the data warehouse.

9. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. The data warehouse and data mining programs is designed to assist RMA in identifying those producers, agents and adjusters that exhibit anomalous behavior.

10. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

Yes. The data warehouse and data mining programs is designed to assist RMA in identifying those producers, agents and adjusters that exhibit anomalous behavior.

11. What opportunities does an individual have to decline, to provide information (i.e., where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses) and how individuals can grant access?

The data used to populate the data warehouse and data mining programs is obtained from FCIC/RMA policyholder database that is populated by data required to be reported by the producer to the Approved Insurance Providers. RMA required data for agent and adjusters is also provided.

12. How will the information be secured (e.g., administrative and technological controls)?

SDAA/CAE secures the data through the RMA VPN, firewalls, virus protection software and password protected data in compliance with, and subject to inspection, by RMA's Security unit.

13. What controls will be used to prevent unauthorized monitoring?

RMA firewall protection, the VPN and RMA security scans prevents unauthorized monitoring.

14. Was the System of Records created under the Privacy Act, 5 U.S.C. 552a?

Yes.

15. Under which Systems of Record (SOR) Notice does the system operate? Provide number and name.

FCIC-10 "Policyholder" record.

16. If the system is being modified, will the SOR require amendment or revision? Explain.

N/A – The system is not currently being modified. If the system was modified, RMA would review the SOR requirements.

APPENDIX A

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL

System Name: SDAA/Data Warehousing and Data Mining

Submitting Office: Garland Westmoreland, Director

1. Privacy Act Applicability Review

_______ Privacy Act is not applicable.

___X____ Privacy Act is applicable. Currently covered under System of Records FCIC-10 "Policyholder" record. No modification to the system notice is required.

_______ Privacy Act is applicable. Needs to create a new system of records.

_______ Privacy Act is applicable. Currently covered under System of Records ______________________________. Modification to the system notice is required. (Attach changes)

Comments:

Language addressing data mining is specifically included in the SOR.

2. Information Collection Applicability Determination

________ No OMB clearance is needed.

________ OMB clearance is needed.

____X___ Currently has OMB clearance.

Comments:

3. System Owner Review and Concurrence

________ Does not constitute a Privacy Act Assessment required by the E-Government Act of 2002.

____X___ Does constitute a Privacy Act Assessment required by the E-Government Act of 2002 and requires approval of the Investment Sponsor.

Reviewer’s Name (Print): Garland Westmoreland
Reviewer’s Signature: **/s/**
Title: Director, SDAA

4. INVESTMENT SPONSOR REVIEW AND APPROVAL OF PIA:

This system collects, maintains, or disseminates personal information in identifiable form about members of the public.

Print Name: James Callan
Signature: **/s/**
Title: Associate Administrator, RMA

5. FOIA/PRIVACY OFFICER CONCUR FOR REVIEW

Print Name: Vondie W. O’Conner, Jr.
Signature: **/s/**
Title: Privacy Officer, RMA

6. INFORMATION SYSTEMS SECURITY MANAGER CONCUR FOR REVIEW

Print Name: Eric Baer
Signature: **/s/**
Title: Senior Agency Information Security Officer, RMA

7. CHIEF INFORMATION OFFICER FOR CONCUR FOR REVIEW AND APPROVAL

Print Name: Vondie W. O’Conner, Jr.
Signature: **/s/**
Title: Chief Information Officer, RMA and FCIC