Risk Management Agency
USDA

Privacy Impact Assessment

For

RMA UNIX and Business Applications

April 2007

Name of Project:
Program Office:
Project's Unique ID:

A. CONTACT INFORMATION:

1. **Who is the person completing this document?**
   Eric Baer, RMA ISSPM
   6501 Beacon Dr, MS 0835
   Kansas City, MO 64133
   (816) 823-1950
   eric.baer@rma.usda.gov

2. **Who is the system owner?**
   Vondie W. O'Conner Jr., RMA CIO
   6501 Beacon Dr, MS 0800
   Kansas City, MO 64133
   (816) 823-4459
   Vondie@rma.usda.gov

2. **Who is the system manager for this system or application?**
   Denise Hoffmann, Director Program Analysis and Accounting Division
   6501 Beacon Dr
   Kansas City, MO 64133
   (816) 926-3406
   denise.hoffmann@rma.usda.gov

4. **Who is the IT Security Manager who reviewed this document?**
   See #1

5. **Did the Chief FOI/PA review this document?**
   Terrie Ray, FIOA
   1400 Independence Ave. SW MS 0801
   Washington D.C., 20250
   (202) 690-5701
   terrie.ray@rma.usda.gov

6. **Did the Agency's Senior Office for Privacy review this document?** (Name, office, and contact information).

7. **Who is the Reviewing Official?**

See #2

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1. Does this system contain any information about individuals?

(a) Is this information identifiable to the individual?

Yes

(b) Is the information about individual members of the public?

Yes

(c) Is the information about employees?

No

2. What is the purpose of the system/application?

This group of applications processes the reinsurance activities of the Federal Crop Insurance Corporation. It contains functions that validate the data received from the Approved Insurance Providers, compare the requests for valid entries, and processes requests for payment.

3. What legal authority authorizes the purchase or development of this system/application?

This system is authorized under the Federal Crop Insurance Act.

C. DATA in the SYSTEM:

1. Generally describe the type of information to be used in the system and what categories of individuals are covered in the system?

The type of information used is that concerning participants in the Crop Insurance Program, their coverage and loss. Also included is insurance agent and adjustor information, financial information from the Approved Insurance Providers (AIP), and other insurance related data.

2. What are the sources of the information in the system?

(a) Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The data is taken directly from the source by the AIP and provided to RMA. RMA does not directly take the data. The data is collected on official FCIC forms.

(b) What Federal agencies are providing data for use in the system?

RMA only.

(c) What State and local agencies are providing data for use in the system?

(d) From what other third party sources will data be collected?

Data regarding agents, adjustors, and the AIP financial data is collected from the AIP.

(e) What information will be collected from the employee and the public?

Typically, the information collected from the public includes name, farm program information (e.g., crops, acreage, etc.), and SSN.

3. Accuracy, Timeliness, and Reliability

(a) How will data collected from sources other than USDA records be verified for accuracy?

There is a validation process that runs when data is input (Data Acceptance System) that validates all information prior to the used by RMA.

(b) How will data be checked for completeness?

The same Data Acceptance System will reject any incomplete information. It is a financial incentive for the AIP to ensure that data transferred to RMA is accurate and complete.

(c) Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

(d) Are the data elements described in detail and documented?

Yes, required data elements are documented in Appendix 3 of the Standard Reinsurance Agreement.

D. ATTRIBUTES OF THE DATA:

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

   Yes. The SSN is required for interaction with Treasury and is specified in the Standard Reinsurance Agreement and the Federal Crop Insurance Act.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

   No.

3. **Will the new data be placed in the individual's record?**

   N/A

4. **Can the system make determinations about employees/public that would not be possible without the new data?**

   No. Although the data received is partially transmitted to the Strategic Data Analysis Data Warehouse for data mining to detect fraud, waste, or abuse, that activity is covered under another PIA.

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

   N/A

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

   The resultant databases are protected by the use of Access Control Lists derived from the operating system.

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

   The processes being consolidated all derive or directly use controls that are inherent to the operating system.

8. **How will the data be retrieved?**

   Data is retrieved using custom Web or client based reports, depending on the group requesting the reports.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Reports can be generated that are for ineligible producers or fro those that owe a debt to the Federal Government.

10. **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)**

An opportunity to decline to give that information is provided on the Privacy Act statement on the Crop Insurance Application.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The system is operated in one site, with the alternate site being restored with data from the primary site. The data at the alternate site is currently a week old.

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

Data is maintained indefinitely for statistical purposes.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

N/A

4. **Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

5. **How does the use of this technology affect public/employee privacy?**

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

Yes. This system will track participation in the Federal Crop Insurance Program. Most data is aggregated for statistical purposes and is not individually identifiable however.

7. What kinds of information are collected as a function of the monitoring of individuals?

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

Access control lists are used to prevent internal abuse or misuse. There is a comprehensive security program that prevents unauthorized external access. This includes access control lists, properly maintained systems, and firewalls.

9. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

FCIC-1:	Accounts Receivable
FCIC-3:	Crop Insurance Actuarial Listing
FCIC-5:	Rejected Applications
FCIC-6:	Insurance Contract Analysis
FCIC-7:	Insurance Contract Files
FCIC-8:	List of Ineligible Producers
FCIC-9:	Agent
FCIC-10:	Policyholder
FCIC-11:	Loss Adjuster

10. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

They system of records notices are being modified to include the use of the CIMS project.

F. ACCESS TO DATA:

1. Who will have access to the data in the system?

Access to the system is granted to contractors (in the role of developers), and Federal Employees that have a specific need to access this specific data in the course of their duties. AIPs have access to data that they submitted.

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

Access is granted by access control lists that are arranged by job function. The supervisor and database/system administrator must approve access.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access is restricted by job function. It is only granted on a least privileged basis.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Users are expected to follow RMA and USDA security and privacy policy. Access is restricted by access control lists and by a layered security approach on the external interfaces of the network (e.g firewalls). An additional firewall separates the General Support System (And hence the applications) from the office automation (Windows General Support System) portion of the network.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**?

Yes. Privacy and non-disclosure language is inserted into the contract. Additionally, they are also expected to abide by RMA and USDA policy regarding security and privacy.

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

Other then the Data Mining, which is a subset of this information, the data is not shared.

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

The privacy rights are protected by the Office of the Chief Information Officer in RMA, which includes the Information Security Branch.

8. **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

The data mining initiative is part of RMA. Some data is shared with the Department of the Treasury.

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

The Treasury data is used to ensure payments to the AIP are processed. Additionally, the Debt Management Application will intercept monies due a producer

(e.g., tax refund) to pay indebtedness to the Federal Government. This data is provided to Treasury.

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

The receiving agency.

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the USDA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

BMA Business Applications / UNIX GSS
(System Name)

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.

Denise Hoffman — 9/19/07
System Manager/Owner
OR Project Representative
OR Program/Office Head. — Date

[signature] — 9/20/07
Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person — Date

[signature] — 9/20/07
Agency OCIO — Date