Privacy Impact Assessment

RMA IT Modernization (ITM)

Revision: 1.5

Risk Management Agency

Date: August 2010

Document Information

Owner Details	
Name	Jon Savage
Contact Number	816-313-4221
E-mail Address	jonathan.savage@rma.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
1.0	6/15/2009	Jon savage	Document Creation
1.1	8/17/2009	Jon Savage	Updated Document Contents
1.2	8/18/2009	Jon Savage	Updated Document Contents
1.3	10/5/2009	Scott Severns	Updated contents
1.5	8/6/2010	Eric Baer	Updated contents to reflect C&A changes

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
Denise Hoffmann	Director Program Analysis and Accounting Division	RMA	denise.hoffmann@rma.usda.gov
Eric Baer	Information Systems Security Program Manager	RMA	eric.baer@rma.usda.gov

Table of Contents

1 System Information

System Information	
Agency:	Risk Management Agency (RMA)
System Name:	RMA IT Modernization "ITM"
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	ITM is a compilation of 60+ web applications that are being developed to replace (modernize) legacy RMA applications/systems.
Who owns this system? (Name, agency, contact information)	Denise Hoffmann, Director Program Analysis and Accounting Division 6501 Beacon Dr Kansas City, MO 64133 (816) 926-3406 denise.hoffmann@rma.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Eric Baer, Information Systems Security Program Manager, RMA 6501 Beacon Dr Kansas City, MO 64133 816-823-1950 eric.baer@rma.usda.gov
Who completed this document? (Name, agency, contact information)	Scott Severns, Information System Security Officer, RMA 650 Beacon Dr. Kansas City MO 64133 816-926-7645 scott.severns@rma.usda.gov

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	The "ITM" system contains records of insured producers' and their policy information, and eligibility determination for participation in RMA and other USDA programs. Included in this information is: Name and tax identification numbers (including social security numbers) of the insured and all persons with a substantial beneficial interest in the insured, the crops insured, coverage levels, price elections, production and yield history; acreage report information including acres, farming practices, planting dates, premium and liability data; a legal description and identification of insured's land; and, if applicable, associated loss data on the insured's land as submitted to RMA by private insurance companies. It also contains SSN and eligibility determinations for participating in RMA programs of agents and loss adjusters contracting with approved insurance providers for sales and service of crop insurance policies, or adjustment of losses.
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 Federal Crop Insurance Act (FCIA) section 506(m) Submission of Certain Information.
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.	Approved Insurance Providers (AIP) provide data to RMA that is collected from Insurance Agents and Loss Adjusters
4.1	What data is being collected from the customer?	Name, Address, Phone Numbers, SSN, EIN number, eAuth ID/Name, Farm IDs
4.2	What USDA agencies are providing data for use in the system?	Risk Management Agency (RMA)
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?	Private insurance companies that are servicing the policyholders

No.	Question	Response
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?	RMA Compliance offices protect the integrity of crop insurance programs through a system of review, analysis, and evaluation to assure laws, policies, and procedures are followed and administered correctly, and to detect and prevent abuse of the crop insurance program. In addition, the policy acceptance and storage system (PASS) contains processes that edit and validate detail policy data submitted by the approved insurance providers to provide reasonable assurance that the data is accurate and timely in accordance with policy, procedure and requirements of the Standard Reinsurance Agreement.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	See Question # 5.1
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	See Question # 5.1

2.2 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?	This data is being collected to determine the eligibility of producers, agents and loss adjusters for the Federal Crop Insurance Program, to detail the amount and types of claims to be processed and/or paid by the RMA on behalf of the FCIC, and to track certain actuarial trends and data to determine viability of current and future insurance products. Certain data is also utilized as the basis for determining expense reimbursement and gain sharing between RMA and approved insurance providers. See The Federal Crop Insurance Act (FCIA) section 506(m) Submission of Certain Information.
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?	Other purposes include sharing data with FSA when used as a basis for eligibility and payment calculations for other disaster programs.

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	☒ 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
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?	RMA Compliance offices protect the integrity of crop insurance programs through a system of review, analysis, and evaluation to assure laws, policies, and procedures are followed and administered correctly, and to detect and prevent abuse of the crop insurance program. In addition, the policy acceptance and storage system (PASS) contains processes that edit and validate detail policy data submitted by the approved insurance providers
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?	RMA documents the intended routine uses of the data being collected in the System of Record Notice (SORN), FCIC Sections 1, 2, 8, 9,10, 11.
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?	Some data will be used within the Comprehensive Information Management System (CIMS)
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.

No.	Question	Response
12.1	What controls are in place to protect the data and prevent unauthorized access?	Operational controls include requiring AIP and their employees, agents, loss adjusters, and any person having access to producer information to Sign Non-Disclosure Statements. In addition, FCIA Section 502(c), prohibits the Secretary, any other officer, employee, or agency of USDA, an approved insurance provider and its employees and contractors, and any other person from disclosing producer-derived information to the public unless it is transformed into a statistical or aggregate form that does not reveal the producer's identity. Technical controls include RMA 'public' WEB sites not exhibiting PII data, requiring AIP to access the public web site through encrypted tunnels, and a number of other additional controls described in the ITM security plan.
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?	Users will not have direct access to the database housing PII information. All users will be utilizing various authorized applications to view PII data. Database schemas have been introduced to segment the data so that an application only gets access to the data it needs to access. Data is accessed via role based authentication on the databases. Unless a user has a specific role on the database server AND a valid active directory account, then there is no way to access the data. Further, sensitive data is encrypted on the database and not displayed on any web based interface. When necessary to be displayed, the data is truncated. The networks and supporting systems are protected via firewalls and actively monitored with intrusion detection systems. (Also See Question # 12.1)

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☒ Yes ☐ No – If NO, go to question 15.

No.	Question	Response
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Due to the necessity to keep data available for possible legal action through the compliance division, all data utilized in the ITM system will be retained a minimum of 25 years. (Pending NARA Approval).
14.2	What are the procedures for purging the data at the end of the retention period?	Procedures for purging data include burning, shredding, deleting, or discarding with other waste materials. In the electronic realm, destruction is typically accomplished by overwriting or degaussing, depending on security requirements.
14.3	Where are these procedures documented?	DR 3080-001 Records Management, Appendix C, Section 6E and RMA policy 10320-001 Media Sanitization Procedures.
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?	. Appendix III of the Standard Reinsurance Agreement establishes data reporting requirements based on program and administrative policy and procedural requirements. It is reviewed and revised annually dictated by policy or procedural modifications, or utilization of data for other administrative determinations according to requirements of the SRA, OIG, GAO, etc.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 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 could be used by FSA for Disaster Payments and Data Reconciliation (required by the Agricultural Risk Protection Act (ARPA)
17.2	Who is responsible for assuring the other agency properly uses the data?	Each agency included in the Memorandum of Understanding (MOU) between RMA, NASS and FSA remain responsible for assuring proper use.
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?	An appropriate Memorandum of Understanding (MOU) between RMA, NASS and FSA exists to ensure appropriate protection of PII and Privacy Act data.

No.	Question	Response
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?	

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	Only authorized users (based on business need) will have access to data within the ITM systems. These users include internal RMA Staff, Management, System Administrators and select Developers on a case by case basis.
21	How will user access to the data be determined?	RMA will determine access requirements according to the ITM operational need and occupational title of the end user.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No
22	How will user access to the data be restricted?	All users will need to submit a formal request to application business owners in order to be granted access to the various ITM applications. RMA Business Managers authorize and configure access via the ITM Security Web Application.
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

2.6 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.)?	The RMA CIO (currently Ken O'Brien), through the FOIA and Privacy office, has overall responsibility to protect PII data.
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	Customers and employees can contact the office responsible for protecting their privacy rights by filing a Freedom of Information Act (FOIA) request.

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.	
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?	The FCIA, regulatory crop policies, ineligible regulations, and FCIC procedures mitigate the risk of depriving participating customers of due process rights.
28	How will the system and its use ensure equitable treatment of customers?	The system ensures equitable treatment of customers by load balancing the database servers and by not collecting any demographic information from customers. The absence of such data helps ensure equitable treatment of customers regardless of national origin, race, gender, and age are not collected and/or stored in the ITM systems.
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	FCIA regulations and procedures provide for eligibility, rate increases and other modifications to the standard coverage issued by FCIC according to farming practices and loss history. The policy acceptance system, CIMS and data mining methods validate or refute the conditions reported by AIPs. Also, the absence of customer demographic data helps mitigate the possibility of treating customers differently based upon their individual or group characteristics.

3 System of Record

No.	Question	Response

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.)?	Records may be indexed and retrieved by the individual or entity name, tax identification number (including social security number), and the private insurance company name, subject of the compliance review or the case number. Data research and analyses records may be indexed and retrieved by State and County, individual or entity name, tax identification number (including social security number), or contract number.
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.)	The system operates under SORNs FCIC-3: Crop Insurance Actuarial Listing FCIC-5: Rejected Applications FCIC-8: List of Ineligible Producers FCIC-9 Agent FCIC-10 Policyholder FCIC-11 Loss Adjuster documented at: http://www.ocio.usda.gov/ocio_sor.html; and http://www.ocio.usda.gov/records/schedules.html)
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

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.
31.1	How does the use of this technology affect customer privacy?	N/A

5 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

RMA IT Modernization (ITM)

(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.

Denise Hoffman
Program/Office Head.

Date

Eric Baer
Agency Privacy Act Officer

Date

Ken O'Brien
Agency OCIO

Date

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

RMA IT Modernization (ITM)

(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.

Denise Hoffman
Program/Office Head.

8/24/10
Date

Eric Baer
Agency Privacy Act Officer

9 Aug 10
Date

Ken O'Brien
Agency OCIO

9 Aug 10
Date