# Privacy Impact Assessment

## Enterprise Support Systems

*Revision: 0*

*Risk Management Agency*

*Date: July 2010*

# Document Information

| Owner Details | |
|---|---|
| Name | Ken O'Brien |
| Contact Number | 202-720-1419 |
| E-mail Address | Ken.obrien@rma.usda.gov |

| Revision History | | | |
|---|---|---|---|
| **Revision** | **Date** | **Author** | **Comments** |
| 0 | 7/23/10 | Eric Baer | Original Document |

| Distribution List | | | |
|---|---|---|---|
| **Name** | **Title** | **Agency/Office** | **Contact Information** |
| | | | |

# Table of Contents

# 1 System Information

| System Information | |
|---|---|
| Agency: | Risk Management Agency |
| System Name: | Enterprise Support Systems |
| System Type: | ☐ Major Application<br>☒ General Support System<br>☐ Non-major Application |
| System Categorization (per FIPS 199): | ☐ High<br>☒ Moderate<br>☐ Low |
| Description of System: | Back-office and network infrastructure support |
| Who owns this system? (Name, agency, contact information) | Ken O'Brien, RMA CIO |
| Who is the security contact for this system? (Name, agency, contact information) | Eric Baer, RMA ISSPM |
| Who completed this document? (Name, agency, contact information) | Eric Baer, RMA ISSPM |

# 2 Data Information

## 2.1 Data Collection

| No. | Question | Response |
|---|---|---|
| 1 | Generally describe the data to be used in the system. | While mostly used for back office support, the system does host the CARS compliance database, and currently processes email. The CARS system is a stand-alone Share Point instance that contains data related to the Compliance program, which includes partial SSNs and program data for certain producers. |
| 2 | Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)? | ☒ Yes <br> ☐ No – If NO, go to question 3. |
| 2.1 | State the law or regulation that requires the collection of this information. | 7 USC 1502 § 501 (Federal Crop Insurance Act) |
| 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 <br> ☐ No |
| 4 | Sources of the data in the system. | RMA Compliance Program and RMA/FCIC insurance documents |
| 4.1 | What data is being collected from the customer? | Name, address, SSN, and other information specified on FCIC insurance documents |
| 4.2 | What USDA agencies are providing data for use in the system? | 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? | 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 <br> ☒ No – If NO, go to question 6. |
| 5.1 | How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness? | |
| 5.2 | How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness? | |
| 5.3 | How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness? | |

## 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? | The principal purpose of the data collection in the CARS application is to investigate potential cases of fraud, waste, or abuse in the crop insurance program. |
| 7 | Will the data be used for any other purpose? | ☐ Yes<br>☒ No – If NO, go to question 8. |
| 7.1 | What are the other purposes? | |
| 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<br>☐ 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<br>☒ No – If NO, go to question 10. |
| 9.1 | Will the new data be placed in the individual's record (customer or employee)? | ☐ Yes<br>☐ No |
| 9.2 | Can the system make determinations about customers or employees that would not be possible without the new data? | ☐ Yes<br>☐ No |
| 9.3 | How will the new data be verified for relevance and accuracy? | |
| 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? | Routine uses include investigation for insurance fraud. |
| 11 | Will the data be used for any other uses (routine or otherwise)? | ☐ Yes<br>☒ No – If NO, go to question 12. |
| 11.1 | What are the other uses? | |
| 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<br>☒ 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? | |
| 13 | Are processes being consolidated? | ☐ Yes<br>☒ No – If NO, go to question 14. |
| 13.1 | What controls are in place to protect the data and prevent unauthorized access? | |

## 2.3 Data Retention

| No. | Question | Response |
|---|---|---|
| 14 | Is the data periodically purged from the system? | ☒ Yes<br>☐ 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? | 7 years from the final disposition of the case. |
| 14.2 | What are the procedures for purging the data at the end of the retention period? | Data is erased from the records management systems |
| 14.3 | Where are these procedures documented? | Share Point site related to the Records management program |
| 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? | Data is reviewed to ensure that it still applies to the case being investigated. |
| 16 | Is the data retained in the system the minimum necessary for the proper performance of a documented agency function? | ☒ Yes<br>☐ 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<br>☒ No – If NO, go to question 18. |
| 17.1 | How will the data be used by the other agency? | |
| 17.2 | Who is responsible for assuring the other agency properly uses the data? | |
| 18 | Is the data transmitted to another agency or an independent site? | ☐ Yes<br>☒ No – If NO, go to question 19. |

| No. | Question | Response |
|-----|----------|----------|
| 18.1 | Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected? | |
| 19 | Is the system operated in more than one site? | ☐ Yes<br>☒ 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.)? | Users that are assigned to the "Compliance role" Each user only has access to their assigned cases. Supervisors may have multiple accesses, but only to the cases of their employees. |
| 21 | How will user access to the data be determined? | RBAC. Permission of the management is necessary to ensure employees are assigned to correct role. |
| 21.1 | Are criteria, procedures, controls, and responsibilities regarding user access documented? | ☒ Yes<br>☐ No |
| 22 | How will user access to the data be restricted? | System and file level permissions |
| 22.1 | Are procedures in place to detect or deter browsing or unauthorized user access? | ☒ Yes<br>☐ No |
| 23 | Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)? | ☒ Yes<br>☐ 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 CARS project manager. |
| 25 | How can customers and employees contact the office or person responsible for protecting their privacy rights? | The details are listed in the CARS SOR, FCIC-2 "Compliance Review Cases" |

| 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.<br>☐ 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:<br>▪ Consolidation and linkage of files and systems<br>▪ Derivation of data<br>▪ Accelerated information processing and decision making<br>▪ Use of new technologies<br>Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)? | ☐ Yes<br>☒ No – If NO, go to question 28. |
| 27.1 | Explain how this will be mitigated? | |
| 28 | How will the system and its use ensure equitable treatment of customers? | The system's use is only to make preliminary determinations. Final disposition is handled by OGC or appropriate legal authority. |
| 29 | Is there any possibility of treating customers or employees differently based upon their individual or group characteristics? | ☐ Yes<br>☒ No – If NO, go to question 30 |
| 29.1 | Explain | |

# 3  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<br>☐ 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 can be retrieved by name. |
| 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.) | FCIC-2 "Compliance Case Reviews" |
| 30.3 | If the system is being modified, will the SOR require amendment or revision? | ☐ Yes<br>☒ 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<br>☒ No – If NO, the questionnaire is complete. |
| 31.1 | How does the use of this technology affect customer privacy? | |

# 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

_____

(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.

_____     _____
System Manager/Owner                              Date
OR Project Representative
OR Program/Office Head.


_____     _____
Agency's Chief FOIA officer                       Date
OR Senior Official for Privacy
OR Designated privacy person


_____     _____
Agency OCIO                                       Date