# Privacy Impact Assessment
## RMA ROE AZURE HVA

**Policy, E-Government and Fair Information Practices**

- Version: 1.0
- Date: June 21, 2022
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

# Privacy Impact Assessment for the

# RMA ROE AZURE HVA

**June 21, 2022**

## Contact Point

**Doug Jones**
**Information System Owner**
**United States Department of Agriculture**
**Doug.Jones@usda.gov**
**816-926-2758**

## Reviewing Official

**Deryl L. Richardson, Jr.**
**FPAC Privacy Officer**
**United States Department of Agriculture**
**deryl.richardson@usda.gov**

# Abstract

The Regional Office Exceptions Systems (ROE) manages the receipt and processing of Exception Requests from regional offices. Provides metadata, rules, and configuration that are used to accept/reject R-records. Creates all the data required to establish premium, liability and indemnity for exception offer publishing it to RMA databases and providing it to the Approved insurance Providers (AIPs).. ROE includes Regional Office Exceptions (ROE), Hybrid Seed, Large Claim Good Farming (LCGF), and Nursery. ROE is hosted entirely on the FedRamp approved Microsoft Government Azure Cloud Software-as-a-Service (SaaS) platform. There are no hardware or software components within the boundary of the system.

# Overview

The Regional Office Exceptions Systems (ROE) manages the receipt and processing of Exception Requests from regional offices. Provides metadata, rules, and configuration that are used to accept/reject R-records. Creates all the data required to establish premium, liability and indemnity for exception offer publishing it to RMA databases and providing it to the AIPs. ROE applications include Regional Office Exceptions (ROE), Hybrid Seed, Large Claim Good Farming (LCGF) and Nursery. (Note that Hybrid Seed, LCGF, and Nursery are separate applications comprised of business products supported by multiple sets of business rules and workflow within the ROE system.)

High level objectives of ROE include:

- Creating a core foundation using Microsoft CRM entities/attributes for the storage of all pertinent RMA data
- Building integration points to capture existing data from 3rd party systems (including PASS)
- Ensuring data integrity
- Utilizing CRM's native security model which grants access to information to specific groups and/or individuals who need it. The security model can be modified in an ad-hoc manner which increases the potential for self-sufficiency
- Engineering a process representative of USDA ROE's business flow by input from USDA ROE team members
- Building a user experience which takes into account the end goal of completing the process in a more efficient manner in addition to capturing data in a consistent fashion
- Gathering data which future metrics will be based on to assist in managerial and executive decision making
- Creating an electronic documentation system to support the USDA ROE process

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law 107-347, 44 U.S.C. §101).

# Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

## 1.1 What information is collected, used, disseminated, or maintained in the system?

Name, Address, Phone Numbers, SSN, EIN number, eAuth JD/Name, Farm IDs

## 1.2 What are the sources of the information in the system?

Business Unit Users provide data to RMA that is collected from Insurance Agents and Loss Adjusters.

## 1.3 Why is the information being collected, used, disseminated, or maintained?

This data is being collected to allow management and processing of Exception Requests from Regional Offices. The application provides metadata, rules, and configuration data that are used to accept or reject these requests.

## 1.4 How is the information collected?

The information is collected via hard copy forms and e-forms completed by the insured producer, insurance agent, or adjustor. The AIP sends this information to RMA on their behalf.

## 1.5 How will the information be checked for 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 to provide reasonable assurance that the data is accurate and timely in accordance with policy, procedure and requirements of the Standard Reinsurance Agreement.

## 1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Federal Crop Insurance Act 7 USC 1501 et seq., Chapter36

## 1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks include the harvesting and misuse of data. They also can be used to put together a rough picture of a producer's operations and finances. In order to mitigate these risks, access to the information is restricted to a valid business need, and further protected by limiting the raw data available. Data is encrypted both during transit and at rest. Records are accessible only to authorized personnel and are maintained in offices that are locked during non-duty hours. The electronic records are controlled by password protection and the computer network is protected by means of a firewall. File folders and other hard copy records are stored in locked file cabinets.

# Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

## 2.1 Describe all the uses of information.

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.

## 2.2 What types of tools are used to analyze data and what type of data may be produced?

The only tools used are COTS office automation products (e.g. Excel) and no derivative data is produced.

## 2.3 If the system uses commercial or publicly available data please explain why and how it is used.

This system does not use commercial or publicly available data.

## 2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

- Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:
  - End users are correctly identified and authenticated according to USDA and FPAC security policies for access managements, authentication and identification controls.
  - Audit logging is performed at the Department-level to ensure data integrity.
- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

# Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

## 3.1 How long is information retained?

Electronic records are maintained indefinitely. Hard copy records are maintained until expiration of the records retention period established by the National Archives.

## 3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records and NARA 36 CFR B - Records Management, Title 7 - Agriculture; Subtitle B-Regulations of the Department of Agriculture

## 3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long-term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures. During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are protected by access control software, physical access controls and if warranted, password-protected.

According to Records Management DR3080-001 Disposition of Inactive Records: Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

# Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

## 4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The data is primarily shared with the RMA Strategic Data Analysis Division. This group performs the forensic data mining of RMA's data, looking for indications of Fraud, Waste, and Abuse.

## 4.2 How is the information transmitted or disclosed?

This data is transmitted via a dedicated VPN line.

## 4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy risks exist during the transmission and storage of the data. The transmission lines are over a dedicated, encrypted VPN to prevent interception and exploitation. Storage of data is mitigated by ensuring the stored data is encrypted.

# Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

## 5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Policy information is shared only with the Approved insurance Providers (AIP). These are the very entities that collect the information. The AIPs use this information for verification of policies they have issued. The AIP's use the Crop Insurance System to collect and provide to FCIC all SSNs or EINs that are required to be submitted by the policyholder under the eligible crop insurance contract, and the SSNs of all employees, affiliates, and other persons as required by FCIC procedures. SSNs or EINs shall be protected, as prescribed in the Privacy Act of 1974 (5 USC § 552a), by the Company and all of its affiliates with access to such information.

## 5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, this information is only shared with the AIPs that collected the information. Collection of data is conducted in accordance with the published SORN FCIC-10 (Policyholder) which identifies: Disclosure to private insurance companies for any purpose relating to the sale, service, and administration of the Federal crop insurance program and the policies insured under the authority of the Federal Crop Insurance Act (Act).

## 5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The data is transferred via an encrypted VPN tunnel. AIP access is controlled via the same 586 identification process as used by RMA.

## 5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The additional risk is minimal as the AIP the data is shared with is the entity that collects the data. The following measures are taken to mitigate the risk of a PII incident:

- All persons who have access to Protected Information or Personally Identifiable Information within CIS, including, but not limited to, personnel, contractors, service providers and affiliates of the Company, shall sign a nondisclosure statement
- In accordance with section 502(c) of the Act (7 US. C. § 1502(c)), neither the Company, nor its personnel, or contractors, or affiliates may disclose to the public any information provided by the policyholder unless such disclosure is otherwise required by Federal law
- The Company and all of its affiliates shall develop, implement, and maintain information controls and systems, including those pertaining to all Protected Information and records, in a manner consistent with the Federal Information Security Management Act (FISMA) (44 USC§ 3541);
- In accordance with the SRA, the Company shall report any loss or unauthorized disclosure of Protected Information or Personally Identifiable Information to FCIC within one hour of discovery of the loss or unauthorized disclosure of such information

# Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

## 6.1 Does this system require a SORN and if so, please provide SORN name and URL.

SORN FCIC-10 (Policyholder) is applicable for this system; this SORN is available at:

https://www.govinfo.gov/content/pkg/FR-2018-12-31/pdf/2018-28375.pdf

## 6.2 Was notice provided to the individual prior to collection of information?

Whenever a user submits their data to USDA, they will be presented with either a privacy statement on a form or portal upon each customer login. The privacy statement serves as notice to the individual, which details the type of information collected, the right to consent to the provide information, and their right to decline to provide their information. Data collected from other applications follow the same data collection protocol.

## 6.3 Do individuals have the opportunity and/or right to decline to provide information?

Upon submission of information via completed form or portal, customer have access to the privacy statement, which details their option and right to decline providing their information to USDA.

## 6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Within the privacy statement on submitted forms and portals, customers review their option to consent to particular use of the information. The privacy statement also contains the SORN and SORN location, that thoroughly explains how USDA uses and shares the information provided. By signing the document, the customer exercises their right to consent to the use of their information. Additionally, the SORN explains that customers may provide written consent when they'd like USDA share their information to a specific entity, that's not already authorized by legal authority.

## 6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Within the privacy statement that is provided for review when customers submit forms and/or complete portal submissions, notice is provided pertaining to what information is collected, the right to consent to provide information, and their to right decline to provide their information. Additionally, the privacy statement contains the location of the associated SORN, which details all privacy concerns and rights pertaining the collected information. For users unaware of the use of their information, a mitigation strategy is customers may contact USDA at any time and be connected to the FPAC Privacy Officer, who will explain the collection and use of their information.

# Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

## 7.1 What are the procedures that allow individuals to gain access to their information?

The privacy statement that is presented to customers upon submission of their information contains the location of the SORN associated with the data collected. The SORN provides instructions to the customer concerning how to gain access to their information. Specifically, the SORN states that individuals may make a written request to the system manager, mailed in an envelope with a letter marked "Privacy Act Request." The statement specifies that the customer must provide their name, address, zip code, name of the system of records, year of the request, and other pertinent information to help identify the file.

## 7.2 What are the procedures for correcting inaccurate or erroneous information?

The privacy statement that is presented to customers upon submission of their information contains the location of the SORN associated with the data collected. The SORN provides instructions to the customer concerning how to correct inaccurate or erroneous information found within their records. Specifically, the SORN states that individuals may make a written request to the system manager with the reason for contesting the accuracy of the information within their record, their proposed amendment to the inaccurate information, and supporting documentation that details how the information is inaccurate or erroneous. The statement specifies that the customer must provide their written statement with their name, address, zip code, name of the system of records, year of the records in question, and any other pertinent information to help identify the file.

## 7.3 How are individuals notified of the procedures for correcting their information?

Upon submission of customer information on forms or via portal submissions, they are provided with a privacy statement. The privacy statement provides the location of the SORN, which acts as the notification to the customers concerning the procedures for correcting their information.

## 7.4 If no formal redress is provided, what alternatives are available to the individual?

If no redress is provided, customers may contact the agency Privacy Officer for any questions concerning their information.

## 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

A privacy risk associated with the redress available to an individual is a third-party request for that individual's information. The risk is mitigated by review of the request to ensure there is proper legal authority for the information to be disclosed.

# Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

## 8.1 What procedures are in place to determine which users may access the system and are they documented?

A least privilege approach is enforced. Users that have write access in development environments may not have write access in production. Access has to be approved by a supervisor and system administrator to ensure that both business need and separation of duties exist. These procedures are documented in RMA Security Policy I 0025.

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.

## 8.2 Will Department contractors have access to the system?

- Yes, Department contractors with a need to know will have access as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements and must obtain Level 2 eAuthentication access
- As part of the FPAC onboarding process, contractors must meet all requirements for access to applications. Through the USDA Rules of Behavior, they are not allowed to download, share, store or print any USDA specific data.
- All roles are approved on a need-to-know basis via FPAC BC management
- Contractors are required to sign NDAs as per the USDA FPAC BC Onboarding process

## 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Once hired, privacy training and security awareness training is completed prior to gaining access to a workstation. The privacy training addresses user's responsibilities to protect privacy data and how to protect it.

## 8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Certification and Accreditation information for this system is:

- FIPS-199 Security Categorization of system: Moderate
- Date initial ATO was granted: TBD
- Date current ATO was granted: TBD
- Date current ATO expires: TBD

This is the initial ATO for this system. Note, however, the application previously was part of the RMA CIS system (CSAM ID# 1870; ATO awarded 8/24/2020; ATO expires 8/24/2023)

## 8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Specific logging of transaction events (including who entered and when the transaction was completed along with type of financial transaction (such as loan activity, program payments, approvals, determinations, general or subsidiary ledger entries, etc.); and application parameter/table changes (such as loan rates, penalties, etc.) occurs as part of the nightly process.

All events are electronic; any paper documents received are converted to electronic records; then the paper documents are maintained behind locked file cabinets or locked doors. Any paper records fall under set RMA records management rules of retention and destruction.

## 8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM. Quarterly access reviews are done to ensure controls are mitigated.

# Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

## 9.1 What type of project is the program or system?

Minor Application.

## 9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. The technology used is all COTS. RMA has built some business rules on top of the COTS, but no real new technology has been developed.

# Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

## 10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes, no 3rd party website (hosting) or 3rd party application is being used.

## 10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

The use of Third Party websites is restricted to generating the Escrow payment amount for an AIP. No PII or financial information is processed by the third party application.

## 10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable.

## 10.10 Does the system use web measurement and customization technology?

Not Applicable.

## 10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not Applicable.

## 10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable.

# Approval Signatures

DOUGLAS JONES

Digitally signed by DOUGLAS JONES
Date: 2022.06.21 10:43:48 -05'00'

Doug Jones
RMA ROE Azure HVA System Owner
United States Department of Agriculture

JAMES FLICKINGER

Digitally signed by JAMES FLICKINGER
Date: 2022.06.21 12:13:24 -04'00'

James Flickinger
FPAC Assistant Chief Information Security Officer (ACISO)
United States Department of Agriculture

DERYL RICHARDSON

Digitally signed by DERYL RICHARDSON
Date: 2022.06.21 10:47:51 -07'00'

Deryl L. Richardson Jr.
FPAC Privacy Officer
United States Department of Agriculture