Privacy Impact Assessment

FPAC DevSecOps Pipeline RMA HVA (Pipeline RMA HVA)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: July 7, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

FPAC DevSecOps Pipeline RMA HVA (Pipeline RMA HVA)

July 7, 2021

Contact Point

Ravoyne Payton
Farm Production and Conservation (FPAC)
Risk Management Agency (RMA)
202-868-3772

Reviewing Official

Darren Nash
FPAC ISSM
United States Department of Agriculture
(816) 926 7198

Abstract

The FPAC DevSecOps Pipeline RMA HVA (Pipeline RMA HVA) is a PaaS platform located in the FPAC AWS GSS environment; this system hosts several RMA High Value Asset (HVA) applications. The Pipeline RMA HVA serves as the security boundary for all former operational RMA HVA applications with a "Low" or "Moderate" FIPS assessment result.

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).

Overview

The FPAC DevSecOps Pipeline RMA HVA (Pipeline RMA HVA) is a PaaS platform located in the FPAC AWS GSS environment; this system hosts several RMA High Value Asset (HVA) applications. The Pipeline RMA HVA serves as the security boundary for all former operational RMA HVA applications with a "Low" or "Moderate" FIPS assessment result. These applications reside on Pipeline RMA HVA:

- Accounting Daily Reports
- Acreage Crop Reporting Streamlining Initiative (ACRSI)
- Actuarial Information Browser (AIB)
- Actuarial Maintenance
- Actuarial Maps Support
- Actuarial Release
- Agent Locator
- AIP Listing
- AIP Resource Land Unit (AIP RLU)
- AIP Setup
- AIP Statistics
- APH Calculator
- Application Control
- CCAVE Services
- CLU Processing
- Compliance Activity and Results System (CARS)
- Comprehensive Information Management System (CIMS)
- Conservation Compliance
- Cost Estimator
- CRDS ETL Processes
- electronic Data Acceptance System (eDAS)
- electronic Records Management System (eRMS)
- Farm Record Lookup Service
- Fiscal Reporting
- Hybrid Seed
- Ineligible Tracking System/Late Payment of Debt (ITS/LPD)
- Insurance Offers Service

- Issues Logs
- ITM Admin Tool
- Job Scheduler
- Livestock Reports
- Map Viewer
- NFC Daily Extract
- Pasture Rangeland Forage (PRF)
- Policy Acceptance and Storage System (PASS)
- Policy Holder Inquiry
- Policy Holder Tracking
- Price Discovery
- Prices
- Producer Policy Service
- Program Performance Assessment (PPA)
- RAS Account Maintenance
- RAS General Ledger Interface (RAS-GLI)
- Recommend Evaluate and Approval Process Support Application (REAP Support Application)
- Regional Office Exceptions (ROE)
- Reinsurance Reports
- Report Render
- Reverse Type 5
- RMA ArcGIS Portal
- RMA File Operations
- RMA Geospatial Tools
- RMA Information Reporting System (RIRS)
- RMA Logging Services
- RMA Notification & Messaging Services
- RMA Security Tools
- Subcounty Services
- Summary of Business (SOB)
- Tobacco Traceability
- Weekend Process
- xPort
- Year End Accounting (YEA)

Pipeline RMA HVA requires the use of PII to perform these functions. The collection of SSN/TINs is authorized by the Federal Crop Insurance Act (7 USC§ 1501).

Pipeline RMA HVA shares data with the RMA Strategic Data Analysis Division, which performs the forensic data mining of RMA's data, looking for indications of Fraud, Waste, and Abuse. Otherwise, data is only shared with the Approved insurance Providers (AIP), the entities that collect the information. The AIPs use this information for verification of policies they have issued.

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?

Approved Insurance Providers (AIP) 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 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. Other purposes include sharing with Farm Services Agency (FSA) when used as a basis for eligibility and payment calculations for disaster programs.

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 an individual'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. Where possible, data is redacted, masked, and/or encrypted.

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 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.

Data is restricted to a valid business need. Where possible, data is redacted, masked, or encrypted. Business need is verified by Agency management, and is restricted to uses for troubleshooting only.

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?

This section only applies to applications that retain records; some applications do not retain records therefore these applications do not have a retention period.

The archiving and retention strategy for applications on Pipeline RMA HVA will be retained in accordance with the NARA Retention Schedule. Information on most applications is retained indefinitely (permanent records).

See Record Retention Policy: https://usdagcc.sharepoint.com/sites/rma-recmgt/FilePlan/Forms/AllItems.aspx?id=%2Fsites%2Frma%2Drecmgt%2FFilePlan%2FOfficial%20RMA%20File%20Plan%20Oct%202020%2Epdf&parent=%2Fsites%2Frma%2Drecmgt%2FFilePlan

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 NARA General Records Schedule Authority. Any deviations from the NARA Retention Schedule will be approved by NARA when the archiving and retention strategy is defined.

https://usdagcc.sharepoint.com/sites/rma-recmgt/FilePlan/Forms/AllItems.aspx?id=%2Fsites%2Frma%2Drecmgt%2FFilePlan%2FOfficial%20RMA%20File%20Plan%20Oct%202020%2Epdf&parent=%2Fsites%2Frma%2Drecmgt%2FFilePlan

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 primary risk is that data could be exposed due to its long storage length. Data is encrypted in the database while "at rest," minimizing the exposure and chance that it can be misused.

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.

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 Pipeline RMA HVA 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.

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 Pipeline RMA HVA, including, but not limited to, personnel, contractors, service providers and affiliates of the Company, shall sign a non-disclosure 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 to 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.

- FCIC-1 Accounts Receivable
- FCIC-2: Compliance Review Cases
- 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-10 Policyholder
- FCIC-11 Loss Adjuster

These SORNS are available at:

https://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

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

Yes, via the enrollment form for crop insurance.

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

Yes

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

No

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.

Notice is given to the individual when they sign up for crop insurance. The risk of not knowing is small, given that the individual has to consent to the collection prior to being allowed to purchase crop insurance.

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?

Individuals are to contact their county office, agent, or AIP for corrections to their data. In rare instances, data corrections can be sent to the RMA FOIA office.

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

Information is sent to RMA via the AIPs in data loads. This ensures that the most accurate data is in the system.

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

RMA notifies the AIP, when necessary, about corrections made. The AIP in turn notifies the individual.

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

There is an appeals process involved to which the individual may apply.

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

Privacy risks are small, but could include disclosure of the information during the appeals process. The PII is not to be used outside of initial setup of the policy and direct transmission to RMA. PII is encrypted during transmission and rest to mitigate those risks.

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

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

Privacy training is provided annually as per Departmental regulations, using the Departmental approved regimen.

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

Yes

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

Database activity monitoring has been implemented. This provides a distinct record of what user/account performed what action on any given database. The networks and supporting systems are protected via firewalls and actively monitored with intrusion detection systems.

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?

Privacy risks include the browsing, illicit downloading, and exposure of data. These risks have been mitigated by placing strict access controls on the data, monitoring of the data and system files for misuse, and the encryption of the data when not in use.

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?

This would be categorized as a D/M/E project according to CPIC rules.

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

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.

None

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)?

No

10.10 Does the system use web measurement and customization technology?

No

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?

No

10.12 <u>Privacy Impact Analysis</u>: 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.

While there is no PII processed or stored in the third party application, security rules are written into the contract to ensure that the security of both systems is maintained. These security rules will be included in the RMA continuous monitoring plan where applicable or reviewed annually. Because there is no PII transmitted to the third party, privacy risk is minimal.

I have carefully assessed the Privacy Impact Assessment for the Pipeline RMA HVA

Agency Responsible Officials

RAVOYNE PAYTON Digitally signed by RAVOYNE PAYTON
Date: 2021.07.14 13:36:14 -04'00'

Ravoyne Payton
Pipeline RMA HVA Information System Owner
United States Department of Agriculture

Agency Approval Signature

DARREN NASH Digitally signed by DARREN NASH
Date: 2021.07.12 14:05:58 -05'00'

Darren Nash
Information Systems Security Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2021.07.12 12:09:05 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture