Interconnection Security Agreement with

{Insert Name Here}

Revision: 1.0

Date: <<Insert Month/Year of Signature>>

United States Department of Agriculture
1400 Independence Ave., SW
Washington, DC 20250

Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only

Document Information

RMA Point of Contact	
Name	
Contact Number	
E-mail Address	
<<Third Party>> Point of Contact	
Name	
Contact Number	
E-mail Address	

Information Security Officer Document Review			
Name/Organization	**Signature**	**Date**	**Comments (if any)**

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

Table of Contents

1 Introduction

This is an Interconnection Security Agreement (ISA) between two parties. The first party is Risk Management Agency (RMA). The second party is <<Insert third party name here>> and hereafter referred to as <<RO Code or Acronym>>.

A system interconnection is defined as the direct connection of two or more information technology (IT) systems identified in this agreement.

2 Connection Purpose

This Interconnection Security Agreement (ISA) covers all applications that implement the interconnection between RMA and << RO Code or Acronym >>.

2.1 System Identification

Name of RMA System:	e.g. Enterprise Applications Services (EAS) Identity, Credential and Access Management (RMA)
Federal Information Processing Standard 199 Categorization:	e.g. Moderate
Authority to Operate (ATO) Date:	
System Owner Name:	
Contact Number:	
Email Address:	

Name of <<RO Code or Acronym>>System:	e.g. Enterprise Applications Services (EAS) Identity, Credential and Access Management (RMA)
Date of last third party certification of security measures:	
System Owner Name:	
Contact Number:	
Email Address:	

2.2 Connection Purpose and Information Shared/Passed

This interconnection provides <<RO Code or Acronym>> a direct connection to RMA's network for the limited purposes of carrying out the Standard Reinsurance Agreement (SRA) between the Federal Crop Insurance Corporation and << RO Code or Acronym >>, which facilitates access to applications and resources used to support delivery of the Federal Crop Insurance Program. The table below lists RMA applications that are available via the interconnection. Access to certain applications are controlled by additional authentication mechanisms. Several of the applications transmit and process personally identifiable information (PII).[1]

[1] As defined in the Standard Reinsurance Agreement, PII means any information about an individual maintained by insurance companies and its affiliates, including but not limited to, education, financial transactions, medical history, and criminal or employment history and

<<RO Code or Acronym>> Access?	RMA Application Name	Application Description	Involves Personally Identifiable Information?
□	ACRSI	Establishes common data elements and automated processes for producers to report common information for USDA programs; simplifies and reduces the reporting burden on producers; and reduces USDA administrative and operating costs by sharing similar data cross participating agencies.	Yes
□	AIP RLU Intake	Receives GeoJson file capturing CLU gap	
□	AIP Batch Statistics	Shows overall processing information for batches submitted to PASS.	
□	AIP Error Statistics	Shows details on records that were in error after PASS processing.	
□	AIP Conservation Compliance	Service endpoint for AIPs to perform a Conservation Compliance status inquiry.	Yes
□	AIP FTP Server	Service to transfer ftp files from one location to another.	Yes
□	Conservation Compliance CRM	Provides an interface for users to submit requests to add, edit and search status of a producer's eligibility for premium subsidy based on conservation compliance.	Yes
□	CARS CRM	Case management system to document and manage fraud investigations and track compliance activities.	Yes
□	SharePoint	Used to facilitate collaboration between RMA and external users in various business and management functions.	Yes

*Instructions: Upon request for direct VPN interconnection or revision, please review the list of applications and select those that the AIP currently and/or is requesting access to through the VPN. If an application isn't on the list, please contact RMA security for additional instructions.

3 Connection Specifics

The interconnection with RMA is accomplished by explicit firewall rules that allow for services to connect to specific <<RO Code or Acronym>> endpoints as depicted Section 12 Interconnection and Endpoint Diagram With Description. Firewall rules will enforce access control through specific IP address(es) and network port(s) as depicted in Section 12 Interconnection and Endpoint Diagram With Description. A direct virtual private network (VPN) tunnel will be allowed to be established between RMA and <<RO Code or Acronym>>.

3.1 Connection Method

RMA will provide authentication and access management capabilities as part of the ISA. Connections from the <<RO Code or Acronym>> to RMA endpoints are always performed over an encrypted TCP/IP or UDP connection. If an SSL\TLS connection is not supported, IPSEC is used to encrypt the communication. Additional specifications of the interconnection can be found in Section 12.

information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

3.2 Connection Segregation

<<RO Code or Acronym>> infrastructure and applications will be sufficiently segregated to ensure a vulnerability cannot be exploited between RMA and the <<RO Code or Acronym>>'s systems. Further, <<RO Code or Acronym>> will ensure that only staff who are authorized access the applications above will have access to the interconnection. All users and administrators will protect the information transmitted in accordance with all required laws, regulations, NIST guidance, and agreements with RMA.

4 Security Controls

Interconnected systems can share various control implementations across respective systems. This often occurs when an application functions within a Major Application (MA) and/or Enterprise Support System (ESS). The MA and/or ESS provides controls to all applications that reside on it. For this interconnection, no controls are inheritable from RMA.

<<RO Code or Acronym>> is responsible for adhering to the information security provisions of the Standard Reinsurance Agreement and its appendixes, including but not limited to the following:

- Standard Reinsurance Agreement Section IV (a) – Information Collection and Data
- Standard Reinsurance Agreement Appendix II Section VI (l) (1) (D) – Security Measures & Third Party Certification
- Standard Reinsurance Agreement Appendix III Section E – Implementing FISMA Information Security Standards and Guidelines

<<RO Code or Acronym>> shall submit data requests made in the information security provisions of the Standard Reinsurance Agreement, its appendixes, and any additional guidance identified by RMA staff.

Any violations of the terms of the ISA by << RO Code or Acronym >> are deemed to be violations of the Standard Reinsuance Agreement.

5 Incident Reporting

<< RO Code or Acronym >> will report incidents in accordance with Federal Policy and Procedures. << RO Code or Acronym >> will keep RMA informed in writing through RMA's designated security officer when incidents occur which might have any impact on << RO Code or Acronym's >> or RMA's systems. These information exchanges will take place as soon as practical to ensure that appropriate steps are taken as soon as possible to mitigate any potential loss/compromise of data or denial of service.

6 Updates/Changes

<< RO Code or Acronym >> will notify and obtain approval from RMA prior to making any tehincal updates or changes to the system architecture that are reasonably expected to impact RMA. RMA will notify << RO Code or Acronym >> of planned technical updates or changes that are reasonably expected to impact << RO Code or Acronym >>. If any of the technical changes significantly affect the security of the systems, << RO Code or Acronym >>agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign

the ISA within one month of implementation. If a new unapproved interconnection, interface, and/or service is detected, it will be refused and documented as a possible intrusion until authorized.

Should a change in the VPN connection specifics identified in Section 11 be warranted, <<RO Code or Acronym>> shall fill out the form in Appendix A and submit to RMA for review and, if approved, implemented. Once a change request is approved by RMA, the change will be attached to the existing ISA and considered approved by all parties noted in Section 13.

7 User Community

Filled out by AIP - Describe the "user community" that will be served by the applications accessed under this interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection.

All persons who have access to data and systems identified in this ISA, including, but not limited to personnel, contractors, service providers and affiliates of <<RO Code or Acronym>>, shall sign a non-disclosure statement to be maintained by the RMA Privacy Officer.

8 Rules of Behavior

All users of either system are required to obtain security awareness training on a regular basis. This agreement does not create any additional training. All users and administrators of <<RO Code or Acronym>> shall protect the information transmitted pursuant to the ISA in accordance with all required laws, regulations, NIST guidance, the Standard Reinsurance Agreement, and instructions from RMA.

<<RO Code or Acronym>> certifies that its systems is designed, managed, and operated in compliance with all relevant agency regulations, official guidance, and policies. To assure compliance and security of each partner organization a thorough review of each organization's System Security Plan (SSP) will be performed.

<<RO Code or Acronym>> will be required to disclose and obtain prior approval of RMA regarding all third party connections. All <<RO Code or Acronym>> persons who been granted authentication credentials to RMA application and systems shall abide by NIST credential protection and utilization guidelines.

9 Audit Trail Responsibilities

<< RO Code or Acronym >> agrees to implement audit and accountability policies and procedures as required by RMA or USDA, as well as federal guidance for proactive and post-incident response efforts., << RO Code or Acronym >> through its respective security points of contact, will provide relevant audit and accountability data to support incident response efforts. At a minimum, <<RO Code or Acronym>> logging activities will include a record of successful and unsuccessful authentication attempts for system resources connected to this interconnection, and must be maintained for a minimum of 30 days.

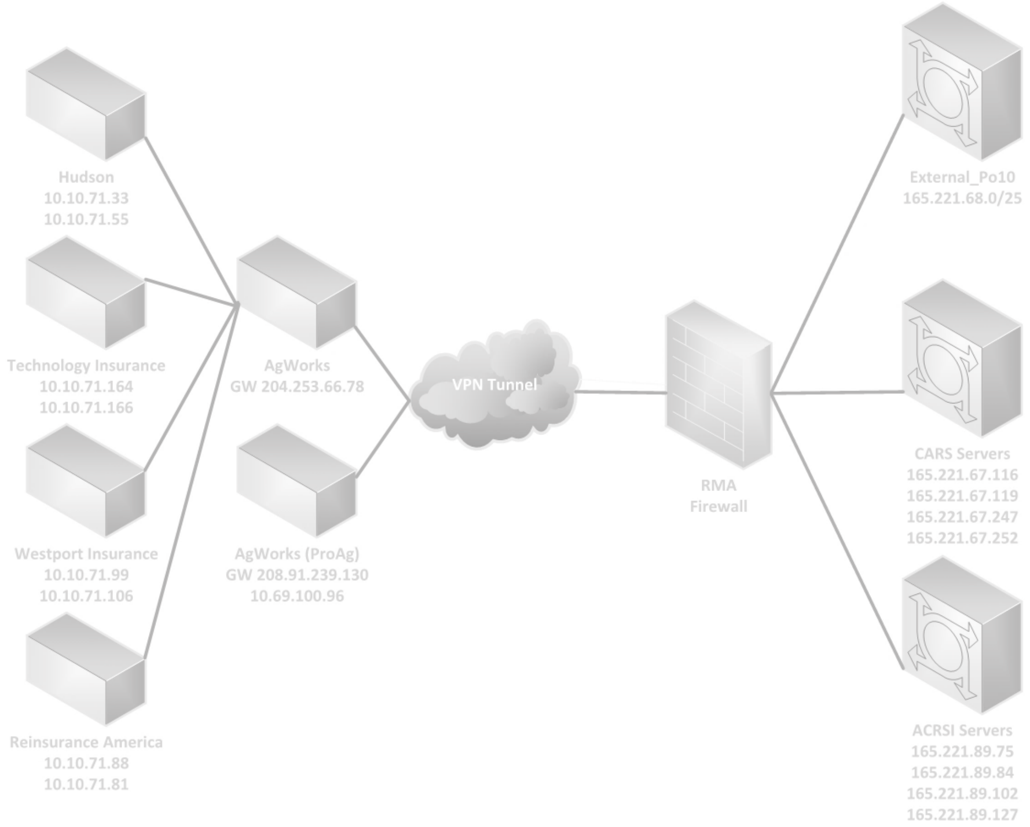
10 Timeline

This agreement will remain in effect for one (1) year after the last date on either Authorizing Official's signature. After one (1) year, this agreement can be continued for an additional two years with concurrence from the ISSPMs for the systems involved. If the parties wish to extend this agreement beyond the three years, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so with 30 days advanced notice or in the event of a security incident that necessitates an immediate response.

11 Interconnection and Endpoint Diagram With Description

The interconnection and endpoint Diagram with Description. RMA and the third party will work together to understand the complete network architecture. Please insert an architectural diagram describing the proposed connectivity.

Below is only an example of the type of detail required for an endpoint diagram:



12 <<RO Code or Acronym>>/RMA Site to Site VPN Specifications

<<RO Code or Acronym>> fills out the following information to initiate a Site-to-Site VPN connection between <<RO Code or Acronym>> with RMA. The information gathered in this section will be used by RMA Network Support to create the connection between RMA and the identified customer below. Once completed, email the entire ISA signed by all relevant parties to RMAITHelpDesk@rma.usda.gov. The subject line should contain "*Site-to-Site VPN Request*".

Customer Technical Contact (*All Fields are Required*)	
Company Name:	
Location:	
Contact Name:	
Contact Email:	
Phone Number (Office or Cell):	
Customer VPN Gateway Information	
Peer IP Address:	
Peer Network List: (*This list should contain sub- networks or specific hosts that need access to the RMA networks. Please include subnet mask of network(s)*)	
Manufacturer:	
Model:	
Software Version:	
RMA Technical Contact	
Contact Name:	RMA Network Support
Contact Email:	ITOBNetwork@rma.usda.gov
Phone Number (Hotline):	816 926-1348
RMA VPN Gateway Information	
Gateway IP Address:	165.221.79.66
Peer Network List: *(This list are the specific sub- networks that will be used to communicate between RMA and Customer site VPN.)*	165.221.64.0 /22 165.221.68.0 /25 165.221.89.0 /24
Manufacturer:	Fortinet
Model:	FortiGate 1000C
Software Version:	5.0 Patch 10

Phase 1 Proposal Policy (*Choose one, if different than Recommendation*)	
Pre-shared Key:	***Key will be provided verbally by RMA Network Support**
Encryption: (*Recommended: AES256*):	☐AES-128 ☐AES-192 ☒AES-256
Authentication: (*Recommended: SHA256*):	☒SHA-256 ☐SHA-384 ☐SHA-512
Diffie-Hellman Group: (*Recommended: 5*):	☐1 ☐2 ☒5 ☐14
Keylife: (*Recommended 86400)*	
Phase 2 Proposal Policy (*Choose one, if different than Recommendation*)	
Encryption: (*Recommended: AES256*):	☐AES-128 ☐AES-192 ☒AES-256
Authentication: (*Recommended: SHA256*):	☒SHA-256 ☐SHA-384 ☐SHA-512
Diffie-Hellman Group: (*Recommended: 5*):	☐1 ☐2 ☒5 ☐14
Keylife: (*Recommended 86400)*	
Comments	

13 Interconnection Security Agreement Authorization

We have carefully reviewed the Interconnection Security Agreement between RMA and <<Insert third party name here>>. This document has been completed in accordance with the requirements set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems. This agreement will be reviewed annually and will be re-signed by all parties every third year.

For RMA

______________________________ ______________

Chad Sheridan DATE
Chief Information Officer

______________________________ ______________

Eric Baer DATE
Information System Owner

______________________________ ______________

Charles Cornelius DATE
Chief Information Security Officer

______________________________ ______________

Michael Alston DATE
Authorizing Official

For <<Insert third party name here>>

______________________________ ______________

<<NAME>> DATE
<<Insert Title of IT Owner>>

______________________________ ______________

<<NAME>> DATE
<<Title of Senior Security Officer>>

______________________________ ______________

<<NAME>> DATE
<<Title of Business Unit Authorizing Official>>

Appendix A: RMA Firewall Change Request Form

This form is to be used for all firewall change request regardless of type (standard or emergency). The information gathered in this form will be used by RMA Network Support to create the firewall access change upon approval from RMA Security. Once completed, email this form to RMAITHelpDesk@rma.usda.gov. The subject line should contain “Firewall Change Request”.

Requestor Contact (*All Fields are Required*)	
Name:	Name
Manager:	Manager
Email:	Email
Phone Number:	Phone Number
Change Information	
Project/Application Name:	Project/Application
Source IP Address: *If more than 1 IP address is required, please list each IP address on a separate line.*	Source IP Address
Destination IP Address: *If more than 1 IP address is required, please list each IP address on a separate line.*	Destination IP Address
Service Port (*please specify tcp or udp*):	Service Port
Service Description:	Service Description
Bi-Directional Connectivity Required *(Yes/No)*:	Yes
Change Type:	☐Standard ☐Emergency ☐Temporary If Temporary, please specify Dates Below: From: From Date to: From Date
Business Justification for Change:	Justification
Comments	

Bi-Directional Connectivity: Requires both source and destination host IPs to originate connections. Normally, the destination host’s reply to an allowed communication from the source host is implied and will be allowed through the firewall without an explicit rule.