Interconnection Security Agreement

& Memorandum of Understanding

Between

Crop Information System (CIS)
&

[AIP System Name]

USDA Risk Management Agency (RMA)

[AIP Company Name]

Revision: 1.0

Date: [Month], [Year]

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

Template Release October 2014

Nondisclosure Statements

All interconnected systems, including those operated by contractor and cloud service providers, shall contain nondisclosure language in the Interconnection Security Agreement (ISA) and Memorandum of Understanding/Agreement (MOU/A) and require a nondisclosure agreement to be signed by all contractors who will access USDA information or information systems. *The Whistleblower Protection Enhancement Act* (WPEA) of 2012, 5 United States Code (U.S.C.) § 2301 et seq. (June 11, 2014) makes it a prohibited personnel practice for Federal agencies to enter into any "nondisclosure policy, form, or agreement" that does not include the following specific language:
"These provisions are consistent with, and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or executive order relating to:
(1) Classified information;

(2) Communications to Congress;
(3) The reporting to the Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or

(4) Any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."

Interconnection Security Agreement Authorization

We have carefully reviewed the Interconnection Security Agreement (ISA) between RMA CIS and [AIP System Name (System Acronym)]. 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.

RMA CIS

Doug Jones	Date

Information System Owner

Lanita Thomas	Date

Information System Security Program Manager

Richard Flournoy	Date

CIS Authorizing Official

[AIP System Name (System Acronym)]

Name	Date
Title	
X	

[AIP System Name (System Acronym)] System Owner (assignment of security responsibility):

Name	Date
Title	
X	

[AIP System Name (System Acronym)] System Security Officer:

Name	Date
Title	
X	

[AIP System Name (System Acronym)] CIO/COO/Director or designee: (responsible executive)

Table of Contents

NONDISCLOSURE STATEMENTS II

INTERCONNECTION SECURITY AGREEMENT AUTHORIZATION 1

1 INTRODUCTION 4

2 CONNECTION PURPOSE 4

2.1 System Identification 4

2.2 Connection Purpose and Information Shared/Passed 5

2.3 Information Sensitivity 6

3 CONNECTION SPECIFICS 6

3.1 Connection Method 6

3.2 Connection Segregation 7

4 SYSTEM VULNERABILITIES 7

5 COMMON/HYBRID CONTROLS 7

6 INCIDENT REPORTING 7

7 BACKUPS/UPDATES/CHANGES 7

8 USER COMMUNITY 8

9 RULES OF BEHAVIOR 8

10 CONTROLS 8

11 AUDIT TRAIL RESPONSIBILITIES 9

12 TOPOLOGICAL/INFORMATIONAL FLOW DRAWING 9

13 TIMELINE. 9

***NOTE TO AUTHOR**: Italicized text throughout this template is provided solely to assist you in creating this document. Please delete all such text prior to submitting this document. In addition, replace all items enclosed in square brackets [ ] with actual information and remove the highlighting.*

1 Introduction

A system interconnection is defined as the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources. The National Institute of Standards and technology's (NIST) ST SP 800-53, Revision 4 Security Assessment and Authorization - Control 3 (CA-3) primarily refers to connections but uses the terms connections and interconnections interchangeably. An interconnection security agreement (ISA) is used to document connections between systems. The ISA is much more than a contract or service agreement between two agencies/departments/divisions/external entities; the ISA is a security agreement that protects both interconnected systems. The ISA details basic system information and documents and agrees on how the security of the two systems will be maintained. Significant benefits that can be realized through a system connection include: reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

2 Connection Purpose

2.1 System Identification

System A:

USDA, Risk Management Agency, Crop Insurance System (CIS)

FIPS 199 Categorization:		**Moderate**
Authority to Operate (ATO) Date:		8/30/2017
System Owner	Name:	Doug Jones
	Contact Number:	816-926-2758
	Email Address:	Doug.Jones@usda.gov

System B:

[AIP Company Name, AIP System Name]

System Owner	Name:	[_____]
	Contact Number:	[_____]
	Email Address:	[_____]

2.2 Connection Purpose and Information Shared/Passed

The RMA Crop Insurance System (CIS) is a series of replacement applications for the legacy UNIX based Crop Insurance business applications. The CIS uses the RMA Enterprise Support System (ESS) as its general support system. The application consists of the following modules (referred to systems by the business community):

- Actuarial Inventory System (AIS) is a replacement for the legacy Actuarial Filing System (AFS). It consists of applications that generate information necessary to sell, administer, and calculate premiums and losses for the crop insurance progrm. It includes processes to calculate, review, analyze, approve, and store: insurance plans; insurance rates; crop prices; crop yields (that form the basis for the insurance offer and policy liability); dates (e.g., planting dates, sales closing dates, contract change dates, billing dates, and other dates necessary for policy enforcement); and Special Provisions of Insurance (SPOI) - statements that attach to the policy and override the basic and crop provisions of the insurance policy.
- These applications support the work that actuaries and underwriters accomplish to maintain current product offerings and create new offerings, ultimately moving the offerings out to the public and private industry partners. These applications are written in ASP. NET, C#, SQL, JavaScript, Linq, and use a SQL Server DBMS.
- A subset of these applications incorporates an Enterprise Geographic Information Systems (GIS) capability to provide a more data rich representation of the information provided to RMA customers/consumers. This includes the ESRI Platform and GIS related software. Current capabilities do not include cloud providers, but that is on the RMA Enterprise Architecture Roadmap.
- The PASS (Policy Acceptance Storage System) module ensures data received is accurate and timely in accordance with the SRA, producer eligibility requirements are met, and errors are corrected in a timely manner. PASS edits ensure AIP data is in accordance with requirements outlined in AIS, FCIC crop policies and procedures, and the Standard Reinsurance Agreement (SRA) and Appendices. This information is the basis for calculation of administrative and operating expense reimbursement and gain sharing with approved insurance providers. PASS also serves as the validation and acceptance point for transfer of company crop insurance information for staging in the RMA.
- There are modules to edit each of the possible 28 record types outlined in Appendix III to the SRA. Current applications are written in ASP. NET, C#, SQL, JavaScript, Linq, and use a SQL Server DBMS. RMA will certainly need maintenance support for these applications, there may be clean-up work and additional functionality to be developed if missed in initial reengineering phases.
- RMA also has a series of global applications overarching all business systems. Some are temporary, such as the Legacy Bridges previously discussed. Some will be

permanent features of the reengineered environment such as Security Umbrella and Tickler/Job Scheduler.

- Corporate Information System consists of reporting applications that provide the end-user community the tools necessary to analyze the current program and make informed decisions regarding possible changes. Intranet applications are used by RMA senior management to monitor the course of the Agency program; by employees' agency-wide to facilitate the work of the Agency; and by compliance investigators, auditors and other trusted reviewers. Sanitized data applications are available to producers, agents, insurance providers and others via the Agency's public website. This system is the reengineered replacement for the legacy Corporate Reporting System. These applications are written in ASP. NET (C#, SQL, JavaScript, Linq, and use a SQL Server DBMS. Again, there may be refining, clean-up work, or additional functionality to be developed under this task order.

2.3 Information Sensitivity

The RMA Crop Insurance System contains the applications for all RMA mission essential functions and ancillary operations in support of the Federal Crop Insurance Act, 7 USC 1501 et seq., Chapter 36. Approved Insurance Providers (AIP) provide data to RMA that is collected from Insurance Agents and Loss Adjusters, to include; Name, Address, Phone number, SSN, EIN number, eAuth ID/Name, and Farm IDs.

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.

3 Connection Specifics

3.1 Connection Method

Connection methods between IP and the Risk Management Agency are limited to SSL and IPSEC VPN connections. SSL VPN connection is a VPN client solution that establishes connection to RMA's front-end firewall. Each client requires a credential login with a password to establish the SSL VPN connection. Site-to-site connections will be established with IPSEC VPN configuration with end points at that AIP and RMA's firewall. Encryption methods will be established at time of creation and be at the highest level available with existing appliances.

3.2 Connection Segregation

In accordance with the Standard Reinsurance Agreement SRA, AIPs will implement Information Security and Privacy controls at a moderate impact security categorization level. At a minimum, AIPs will implement the Basic Security Requirements outlined in NIST SP 800-171. NIST SP 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, and recommends specific security requirements to achieve that objective. The basic security requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

4 System Vulnerabilities

One system's vulnerabilities can have an adverse impact on the security of another system, especially when the two systems are connected and sharing information. Because of this, the system owners and the security officers must be aware of the identified vulnerabilities of all the systems that are connected to their system.

POA&M's for CIS are retained in CSAM.

POA&M's for [AIP System Name (System Acronym)] are submitted to FPAC-BC in accordance with the SRA.

5 Common/Hybrid Controls

The two systems outlined in this ISA share data; therefore, this section and the appendix are not applicable.

6 Incident Reporting

Suspected or confirmed loss of Controlled Unclassified Information (CUI) or Personally Identifiable Information (PII) shall be reported to RMA within 1 hour of discovery in accordance with the order of precedence stated in the SRA.

Within 24 hours after submitting an initial report, AIPs will submit an Agricultural Security Operations Center (ASOC) Form AD 3038, ASOC PII Incident Report to the RMA Cybersecurity Team @ RMA.Security@rma.usda.gov. The AIP will send updated reports periodically until the incident is closed with ASOC.

Each Organization agrees to provide proactive and post-Incident response efforts.

7 Backups/Updates/Changes

Full system backups are weekly and differential/incremental backups are completed daily. The backups are retained on infrastructure disks then migrated to Azure cloud storage.

Changes to production systems go through a formal change management process. This process documents and communicates the planned changes and requires rigorous testing and approvals from key stake-holders before implementation. Contingency plans for backing out a change must also be submitted as part of the process. Where ever possible, deltas are scripted for consistency when promoting changes in code, configuration and data from development through test, and ultimately to production.

8 User Community

Approved Insurance Providers (AIPs) use the interconnection to ensure AIP data is in accordance with requirements outlined in AIS, FCIC crop policies and procedures, and the Standard Reinsurance Agreement (SRA) and Appendices. This information is the basis for calculation of administrative and operating expense reimbursement and gain sharing with approved insurance providers. PASS also serves as the validation and acceptance point for transfer of company crop insurance information for staging in the RMA.

All users are required to have standard background investigations and complete annual security awareness training.

9 Rules of Behavior

Users are bound by USDA policy and guidelines. USDA employees and contractors are required to complete the annual USDA Security Awareness Training and pass a background investigation. The system security controls must be enforced, and audit logging must be enforced.

No new or additional security awareness or training requirements are needed as a result of implementing the interconnections between the systems identified in this agreement.

All users and administrators are expected to protect the information transmitted in accordance with all required laws, regulations, and NIST guidance.

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant agency regulations, official guidance, and policies. As part of assuring this compliance for the security and benefit of each partner organization, thorough review of each system's SSPs, has been performed.

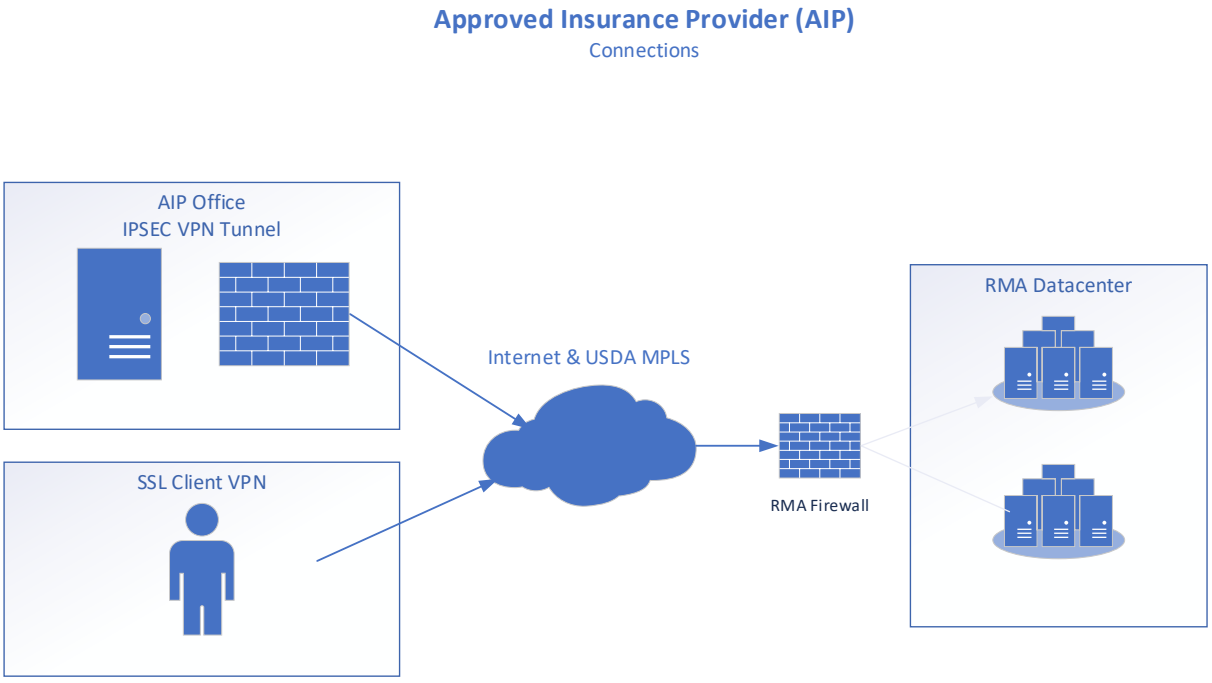
10 Controls

There are no special controls to be inherited specific to the interconnectivity between RMA and the AIPs.

11 Audit Trail Responsibilities

RMA and AIP's agree to implement audit and accountability policies and procedures as required by USDA and Federal guidance (i.e., FIPS 200) for proactive and post-incident response efforts. Where agreed upon in writing, each organization through their respective ISSPMs, will provide relevant audit and accountability data to support incident response efforts.

12 Topological/Informational Flow Drawing



13 Timeline

This agreement will remain in effect for one (1) year after the last date on the Authorizing Official's or CIO/COO/Director or designee's signature. After one (1) year, this agreement can be continued for an additional two years with concurrence from the ISSPM and AIP system owner 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 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.