Privacy Impact Assessment
MRP Azure Cloud GSS

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: December 4, 2019
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

MRP Azure Cloud
General Support System

December 9, 2019

Contact Point

Marco A. Munoz
MRP Azure Cloud System Owner
USDA/APHIS/MRP-IT
970-494-7140

Reviewing Official

Tonya G. Woods
APHIS/MRP Privacy Act Officer
(301)-851-4076

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Marketing and Regulatory Programs (MRP) Azure Cloud General Support System (GSS). The MRP Azure Cloud GSS provides cloud based information technology services for the MRP agencies for compliance requirements and information technology modernization efforts. This PIA was conducted because the MRP Azure Cloud GSS has the potential to store personally identifiable information within the system.

Overview

The Animal and Plant Health Inspection Service (APHIS) is charged with protecting and promoting U.S. agricultural health, regulating genetically engineered organisms, administering the Animal Welfare Act and carrying out wildlife damage management activities. These efforts support the overall mission of USDA, which is to protect and promote food, agriculture, natural resources and related issues. APHIS is charged with supporting the information technology needs for the USDA MRP mission area agencies which includes APHIS and the Agricultural Marketing Service (AMS). AMS is charged with administering programs that create domestic and international marketing opportunities for U.S. producers of food, fiber, and specialty crops, and delivering services to the agriculture industry that ensure the quality and availability of wholesome food for consumers across the country.

The purpose of this system is to provide supporting information technology services to employees Marketing and Regulatory Programs that facilitates domestic and international marketing of U.S. agricultural products and ensures the health and care of animals and plants.

The MRP Azure Cloud is a mission area GSS for cloud based infrastructure and platform services for the AMS and APHIS agencies.

The APHIS MRP Information Technology (IT) organization established an infrastructure cloud environment through the use of the Microsoft Azure Government cloud services. Connectivity to these services is through a private network connection between the USDA network and Microsoft datacenters used for government customers. The system is comprised of major components providing a multitude of services to MRP agency employees and program units from AMS and APHIS. The services include machine virtualization, storage, networking, application platforms and other cloud based services from Microsoft. The cloud service provider, Microsoft, is responsible for and provides the physical and cloud service foundation that the system components are built on. For a complete list of components in the GSS, please see the narratives in the SSP.

The Azure Cloud GSS has components which process, collect, or retain information on USDA employees, contractors or other entities working on behalf of USDA. The system provides the infrastructure and services for MRP agency program units that store information that may contain PII and/or privacy data.

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?

The GSS stores data used and processed by a number of MRP agency programs in the course of fulfilling their mission for USDA. It is expected to hold any type of data AMS and APHIS uses for applications or general services. The boundary of the data stored is the responsibility of the application/investment including the SORNs and privacy impacts. The GSS maintains the data and is responsible for the security of the stored data.

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

The source of information that resides within the GSS will be from users and other major applications for which a PTA/PIAs has been written. In addition, the stored information is for AMS and APHIS employees/contractors in support of the mission of the MRP agencies.

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

It is for the mission work of MRP agencies that include internal and external sources. This includes contractor numbers, employee name, and home telephone numbers. It may also include the potential for users or systems to store documents and/or data that is extracted from other applications to support the purpose or function of their application or system operating in the GSS boundary. An example of this is data being transferred from another authorized system existing in a different data center to a resource provisioned in the GSS where it is process by a program unit's application for a particular business function.

1.4 How is the information collected?

The information is obtained through the course of fulfilling the mission of the MRP agencies. MRP agencies and program units operate applications and/or systems which may collect information. Those applications are managed as a separate system, as a separate security boundary, that would detail how information is collected for their specific need. This includes establishing a separate PTA and PIA. These applications can operate within the boundary of the GSS and run using offered services.

1.5 How will the information be checked for accuracy?

The data is checked for accuracy by the MRP agency employees collecting the information. The GSS maintains information through the storage components and applications maintained on the system. Each application system owner is responsible for documenting the data about their system within their own boundary documents. In some cases, applications developed or used can provide assistance with data validation and accuracy checking. The GSS maintains the security of the data and applications servers or services. The GSS does not collect information instead it maintains the information needed to support the mission of the agency.

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

The GSS does not collect information. However, the legal authorities defined in the collection of information by MRP agencies' program units operating applications and systems include, but are not limited to the following:

Agriculture Improvement Act (Farm Bill);

Animals and Animal Products (CFR Title 9);

Animal Damage Control Act;

Animal Health Protection Act;

Animal Welfare Act;

Defense of United States Agriculture and Food (HSPD-9);

Food and Drugs (Title 21 U.S.C)

Plant Protection Act;

Public Health Security and Bioterrorism Preparedness and Response Act; and

Virus Serum Toxin Act.

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

Risks are identified via findings, audits & incidents (see below). Once identified, they are mitigated based on the vulnerability criticality. If the timeline exceeds 30 days, a cost worksheet and Plan of action & milestone (POA&M) are approved by the system owner.

Since FY18, no privacy risks were identified for the Azure system. If a privacy risk is identified in the future, Azure stakeholders, will work with various teams, and the Privacy Office, to remediate vulnerabilities. If the risk has been identified as a PII breach, it will be reported within one hour of the incident, to USDA Cyber Security Officials.

Risk Source Findings

- OIG Audit
- GAO Audit
- FFMIA/FMFIA
- FDCC/USGCB
- Incident (privacy breach)
- DHS Finding
- Cyber Stat/PIV
- FISMA A&A

Possible Privacy Risks

RISK	Mitigating Factors
Integrity and availability of data	The risks are mitigated through the use of 2 factor authentication. Azure cloud services have storage redundancy, geo-regional duplication, security access controls and encryption to protect GSS data from corruption and loss of access.
Privacy rights of customer/employees	All access to the system would require authentication by authorized personnel only. Application access limits access to relevant information and prevents access to unauthorized information. Any privacy information and information in general will have multiple layers of security protecting customers/employees if data is stored.
Data encryption	Use of DLP technology, firewalls, IDP/IPS technology, proxy servers is used for data protection. Azure cloud services enable the GSS to encrypt data at rest while additional means for operating systems and databases will add further encrypting capabilities using Bitlocker for storage and Transparent Data Encryption.

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.

The information stored is used to carry out the mission of MRP agencies.

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

Not Applicable. However, based on requirements of work to be performed by the MRP agencies, employees and contractors, the use of varying tools, applications and cloud services may be deployed to work with data stored in the GSS. Agency programs may generate additional work product data based on their needs and requirements to address the mission of MRP agencies.

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

Not Applicable. The system itself does not use commercial or publicly available data. However, the GSS enables agency programs to store data that may originate from commercial or public suppliers to perform the mission of MRP agencies.

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.

The GSS does not collect. However, it is a platform used to save data. The infrastructure has implemented controls to secure the data stored locally for the support of the MRP agencies.

The GSS uses two-factor authentication to access and use role based access controls to operate and manage the system. Any application operating within or use the GSS will conform to access, authentication and authorization requirements meeting security and configuration standards and mandates. The degree of information handling compliance will be based on program, application and compliance requirements. The GSS enables the proper handling of information based on specified requirements (see below).

- Authority & Purpose
- Accountability, Audit Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

The GSS has capabilities to automatically protect data of the GSS by default include automatically encrypting data at rest and denying access by default. The storage

system automatically encrypts data stored. Access controls are enabled. They include such items as firewalls denying all traffic by default at three different key points in the network before there is access to the applications and their data storage. Additional means for locking down application resources for further protections are possible. In cases such as this, it is dependent on a program unit's application or system specified requirements.

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?

Items are retained per the General Records Schedule 24: Information Technology Operations and Management Records, records are destroyed based on the subject matter.

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

Each of the program offices that collect data will schedule the records as required.

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

As of FY20, no risk have been identified.

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?

This is based on the programs use of the data and this would be documented in their appropriate PIA and/SORN.

4.2 How is the information transmitted or disclosed?

This is based on the programs use of the data and this would be documented in their appropriate PIA and/or SORN.

The GSS offers means of protection for program unit data. This comes in the form of encrypted transmission, encrypted storage, support for encryption protocols and access controls.

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.

Not Applicable.

The GSS enables information sharing or has components being used by program units for their business needs, systems or application. Privacy risks are mitigated use of security controls for authentication, authorization functionality, segregation for data and network access controls.

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?

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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.

Not Applicable. Each program will create and publish a SORN for the data they are responsible for.

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

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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

Not Applicable.

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.

No. SORNs are the responsibility of the programs. Each program will create and publish a SORN for the data they are responsible for.

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

No PII is collected by the GSS. The infrastructure stores the information collected by the programs. Notice is the responsibility of the programs.

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

Not Applicable.

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

Not Applicable.

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.

There is no risk identified with individuals not being unaware of the collection of data.

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 procedures to allow individuals to gain access to their information is documented in the appropriate PIA and or SORN. That is the responsibility of the programs.

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

Procedures are established within the programs.

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

The information is provided in the appropriate PIA and/or SORN. This is the responsibility of the programs.

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

Not Applicable.

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

There are no identified risks associated with the redress.

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?

Rules of Behavior (ROB) is implemented for which all GSS users, including privileged users, must consent prior to being granted system credentials for access. The GSS inherits the USDA implementation of User Security Awareness training which is provided annually by the Department. MRP IT has created access control lists

(ACLs) and uses role based access controls (RBAC) for the GSS that determine who within agencies can access system resources. Authorization for access to these secured resources must be obtained before a user is granted access.

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?

The Department's IT Security Awareness Training Program is provided on an annual base and is mandatory for all MRP employees. All users are required to sign a ROB that addresses privacy related responsibilities. Employees also have to take privacy training, to ensure they know how to address PII, breaches, and retention.

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

Yes. The system received an approval to operate (ATO) 11/23/2018. The FISMA A&A will be conducted on an annual basis, until the ATO expires 11/23/2021.

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

All users are required to have an individual user account to access the GSS. Firewalls and intrusion detection systems prevent unscrupulous parties from accessing the GSS.

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?

Not Applicable.

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?

The system is a General Support System (GSS).

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

No, the GSS does not employ technology which may raise privacy concerns.

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?

Not Applicable. The GSS does not use third party websites or applications.

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

Not Applicable. The GSS does not use third party websites or applications.

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

Not Applicable. The GSS does not use third party websites or applications.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?

Not Applicable. The GSS does not use third party websites or applications.

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

Not Applicable. The GSS does not use third party websites or applications.

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

Not Applicable. The GSS does not use third party websites or applications.

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?

Not Applicable. The GSS does not use third party websites or applications.

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. The GSS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not Applicable. The GSS does not use web measurement and customization.

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. The GSS does not use web measurement and customization.

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. The GSS does not use third party websites or applications.

Approval Signature

JANELLE JORDAN
Digitally signed by JANELLE JORDAN
Date: 2020.01.15 14:16:14 -05'00'

Tonya Woods
APHIS/MRP Privacy Act Officer (PAO)
Animal and Plant Health Inspection Service
United States Department of Agriculture

PRESTON GRIFFIN
Digitally signed by PRESTON GRIFFIN
Date: 2020.01.17 13:44:03 -05'00'

Preston Griffin
MRP IT –Information System Security Program Manager (ISSPM)
Animal and Plant Health Inspection Service
United States Department of Agriculture

MARCO MUNOZ
Digitally signed by MARCO MUNOZ
Date: 2020.01.16 14:53:31 -07'00'

Marco A. Munoz
MRP IT – MRP Azure Cloud GSS System Owner
Animal and Plant Health Inspection Service
United States Department of Agriculture