Privacy Impact Assessment
APHIS Geographic Information System (GIS) Cloud

- Version: 1.0
- Date: January 12, 2017
- Prepared for: USDA OCIO TPA&E

Privacy Impact Assessment for the

APHIS GIS Cloud

January 12, 2017

Contact Point
Patrick J. McFall
USDA APHIS MRPBS ITD
970-494-7214

Reviewing Official
Tonya G. Woods, APHIS-LPA
APHIS Privacy Officer
United States Department of Agriculture
301-851-4076

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection Service Enterprise Infrastructure Geographic Information System (APHIS GIS Cloud) within the ESRI Cloud environment. The APHIS GIS Cloud provides the connectivity platform for APHIS programs to use GIS services within a Cloud environment. APHIS uses geographic information system (GIS) in the field and office environments to conduct animal and plant surveys, sampling, monitoring, analysis and reporting. The use of GIS data and analysis has become an integral part of how APHIS conducts businesses.

This PIA was conducted because the APHIS GIS Cloud has the potential to store personally identifiable information within the file servers in the ESRI Cloud environment.

Overview

The Animal and Plant Health Inspection Service (APHIS) is responsible for protecting and promoting U.S. agricultural health, administering the Animal Welfare Act and Horse Protection Act, and carrying out wildlife damage management activities. The APHIS mission is an integral part of the U.S. Department of Agriculture (USDA) efforts to provide the Nation with a safe and affordable food supply. APHIS guards against the introduction, reemergence and spread of animal and plant pests and diseases that could limit production and/or damage export markets. Without this protection, threats to our food supply and our nation's economy would be enormous.

As part of our protection focus, APHIS monitors for and responds to emergencies of varying types and scopes. APHIS is classified as an Emergency Response Agency. The Agency also responds to conflicts between humans and wildlife, addresses trade barriers related to animal and plant health, promotes the humane treatment of animals covered by the Animal Welfare Act and Horse Protection Act, and ensures that biotechnology-derived agricultural products are safe.

Geographical Information Systems (GIS) are a critical tool for improving the quality, accuracy, and responsiveness of services provided to APHIS personnel and stakeholders dependent upon services that APHIS provides. Within APHIS there are many different levels of GIS expertise and most departments within APHIS currently invest significant resources in maintaining and creating GIS data sets and systems. Leveraging resources and coordinating policy through a collaborative effort would increase the accuracy, cost-effectiveness, and comprehensiveness of geospatial information in APHIS.

An agency wide enterprise approach to Geospatial technology will optimize the efficiency and effectiveness in the use, acquisition, and dissemination of Geospatial resources. This will increase the cost-effectiveness, innovation, reliability, accuracy, and value of geospatial information and tools, leading to improved outcomes and enhanced services within APHIS.

APHIS currently relies on desktop GIS computing, this limits the ability to share or collaborate on projects within the Agency and also within individual programs. Within APHIS, Plant Protection and Quarantine (PPQ), Veterinary Services (VS) and Wildlife Services use limited server-based GIS, with little to no cross program integration. USDA also has a cloud platform for sharing GIS data in a FISMA low environment, ArcGIS Online (AGOL), which does not provide the ability to collect, share, or analyze data that may be more sensitive. The workflow to use AGOL is labor intensive to manage the data shared on this platform.

This project moves the current APHIS GIS to the Environmental Systems Research Institute, INC (ESRI) FedRAMP Moderate compliant Cloud environment. GIS services will reside in the Cloud for

use by various groups within APHIS. In making this change, APHIS will look for the use of industry best practices to develop a system that is secure, scalable, reliable, cost-effective, and efficient in its use of APHIS resources.

APHIS uses geographic information system (GIS) in the field and office environments to conduct animal and plant surveys, sampling, monitoring, analysis and reporting. The use of GIS data and analysis has become an integral part of how APHIS conducts businesses.

The implementation of ArcGIS online (AGOL) and Portal for ArcGIS (Portal) at the APHIS level would afford programs the ability to streamline the collection and use of GIS data and provide the ability to further evolve GIS practices to enhance the effectiveness of the APHIS programs. Using Portal APHIS staff will be able to plan and conduct operations based on the boundaries of our partner's properties who we have entered into agreements with. It will also allow APHIS programs to better collaborate internally, by recording the location of all of our equipment (traps, trail cameras, and other devices) staff members can assist each other in checking traps or removing devices from the field through a mobile map centric collection platform. Portal will also provide a means for sharing and storing data for both operational support and research collaboration.

Cloud-based GIS would enable us to move away from developing maps that must be reviewed, finalized, and then emailed to our customers. A centralized, web map application would be extremely beneficial in developing maps for emergency response, as shown in the attached use case slides. A cloud GIS solution for emergency mapping enables "non-technical" responders with dynamic and accessible map tools for quick, daily map reporting.

In other areas, cloud GIS allows APHIS to utilize tools, such as ESRI Maps for Office (EMFO) for "self-service GIS". Map tools embedded within Excel (part of the EMFO) provide basic map and analytical tools for our veterinary epidemiologists and VS staff. EMFO leverages either ArcGIS On-line (AGOL) or Portal (the more secure, on site solution) to provide these tools within Excel.

In addition, APHIS plans to migrate disease reporting into the cloud GIS environment. APHIS program staff currently develops maps for disease reporting for many program diseases; including but not limited to: Chronic Wasting Disease, Swine Enteric Corona Diseases, and others.

Cloud based GIS disease reporting would provide a means to central disease reporting tools, increase flexibility in customizing reports, and streamline delivery of final map products to our customers.

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 APHIS GIS Cloud potentially stores data used and processed by a number of APHIS applications.

APHIS collects or receives data from agriculture producers, state agriculture authorities, Federal agencies, and other third parties about land properties, practices, and animal health. This data is used to create information products to assist with protecting the health of commercial, private,

or natural resources in the U.S. This information may include following: name, address, phone number, crop/crop strain/variant, livestock, livestock disease, diagnostics results, invertebrate pests present, national premise identification number, program premises identification number, associated flock/herd identification numbers, photographic image/identifying characteristics, tag distribution records, inspection records, crop/host information, wildlife conflicts, photographic images and geospatial properties of all of the above.

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

- Veterinary Services Emergency Management Response System (planned)
- Veterinary Services Comprehensive and Integrated Animal Health Surveillance System (planned)
- Wildlife Services Management Information System 2000
- Plant Protection and Quarantine Integrated Plant Health Information System

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

APHIS uses geographic information system (GIS) in the field and office environments to conduct animal and plant surveys, sampling, monitoring, analysis and reporting.

1.4 How is the information collected?

The present use of the system does not include interconnections. The information will be entered into the system by GIS professionals and the information will be collected by the IT system in the respective program.

The future use of this system includes interconnections and the information will be by various means including field data collection by state and federal agriculture authorities working with stakeholders, direct observations by APHIS employees, through contractors, or by other means that will be determined. The data will be processed through enterprise data collection systems, including, web-forms, secure mobile devices, paper forms, or any other agency approved means.

1.5 How will the information be checked for accuracy?

Accuracy will be insured by commercial off the shelf software (COTS) through the platform, standardized collection methods with business rules in place, and post collection methods including electronic data transfer procedures and manually viewing and correcting errors through standardized, scheduled, and ad-hoc procedures specifically designed for enterprise data quality.

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

The following legal authorities require collection of certain information will vary depending upon the application used. The following are some examples of legal authority:

- The Animal Health Protection Act, 7 USC 8301-8317

- 7 U.S.C. Section 7629 and 8791
- The Farm Security and Rural Investment Act of 2002
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002 116 Stat 674-678
- The Act of March 1931 as amended (46 Stat; 7USC 426-426b/c)
- Debt Collection Improvement Act of 1996
- Plant Protection Act 7 USC 7701-7786
- The Honey Bee Act 7 USC 281-286
- The Food conversation and Energy Act 2008

In addition, WS enters into agreements with cooperators in the private and public sectors in which such cooperators agree by signature to submit the information collected. The agreements include Memoranda of Understandings, Memoranda of Agreements, Cooperative Service Agreements, and Cooperative Service Field Agreements.

- 9 CFR
- Animal Welfare Protections Act

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

The privacy risks identified would be:

RISK	Mitigating Factors
Integrity and availability of data	The risks are mitigated through the use of 2 factor authentication.
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
Data at rest is not encrypted	DLP technology, firewalls, proxy servers

2 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.

Information in this system will be used in performance of daily field work, in making management decisions, predicting the spread of disease, during emergency management, in the process of the investigation of genetically engineered organisms, epidemiological or other field

investigations, analytics, and to inform internal stake holders of work being performed by APHIS personnel and agency locations.

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

Various tools may be used to analyze the data, most of which will be COTS tools developed by ESRI, analysis that may be done but not limited to overlays, statistics, geostatistics, spatial analysis, and predictive modeling.

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

Publicly or commercially available data that may be used includes but is not limited to agriculture populations, parcel boundaries, public land boundaries, political boundaries, cadastral features, feature location (such as cell towers, buildings, bridges, etc…), water boundaries, ports, habitat distribution models, climate, service premises (landfills, incinerators, and renderers), and roads.

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.

All systems are carefully designed using role-based security models that only allow users access to data need to complete their work.

Interconnectivity Service Agreements will be established to for electronic records integration between the APHIS GIS Portal and systems listed in section 1.2.

Also, to protect privacy and confidentiality of producer data all reporting included standardized templates with disclaimer about appropriate use of the data.

All APHIS users complete computer security training on an annual basis which included data and information security principles.

APHIS has a FOIA office that evaluated the proper release of information for FOIA requests.

3 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?

Data retention will vary depending upon the system and the type of information received. APHIS will follow the Records Management regulations as required.

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

MRP400 will be submitted to Agency records officer for submission to NARA for approval.

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

Retention of the data is required to meet business and organizational requirements for this information system. The retention time will depend upon the type of data stored and will ensure alignment with retention of other government records which may be used to support civil or criminal prosecutions (i.e., based on the Statute of Limitations.) The risk of unapproved release of GIS data outside of the system. All requests for access to GIS data, both internally and externally, would be approved by the GIS Data Management System Owner and/or Administrator/Manager to ensure compliance with the policy prior to the release. APHIS' current systems security measures would mitigate the risk of unapproved access to GIS records.

4 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?

Data may be shared with USDA Office of General Counsel if legal processes, especially litigation actions are brought to by APHIS, its programs or by entities in the private sector. Other investigatory units within USDA may be provided access to some data if an investigation of waste, fraud, or abuse, or investigation of misconduct by an APHIS employee is implemented.

Data sharing will depend upon the application that uses this platform. The individual application PTA/PIAs will reflect any additional data sharing activities. All data shared or disseminated will follow Federal and Departmental regulations and/or laws regarding the protection of the data.

4.2 How is the information transmitted or disclosed?

Information transmitted or disclosed by USDA is provided through the APHIS Privacy Officer in a format or processed defined by the Department in conformity to USDA information disclosure and transmittal procedures.

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.

There is a risk that the data may be shared in an unauthorized manner. To mitigate this risk, detailed reports with personal information are marked "FOR OFFICIAL USE ONLY". Data are analyzed by APHIS staff who are trained in the proper use and dissemination of the data sets. Data in the applications are constrained by roles and privileges designed to prevent the unauthorized access of data.

5 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?

APHIS may share information with other Federal and State government officials, employees, or contractors when necessary to carry out the mission. The type of data sharing will depend upon the application that uses this Cloud service. Data sharing will depend upon the application that uses this platform. The individual application PTA/PIAs will reflect any additional data sharing activities. All data shared or disseminated will follow Federal and Departmental regulations and/or laws regarding the protection of the data.

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.

Information shared and transmitted containing PII would depend upon the application using the GIS cloud.

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

Data shared on maps is distributed through descriptive reports, presentations, stakeholder announcements, or made available on the APHIS website or shared through email distribution.

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

A potential risk to information resulting from external sharing would be transmittal of unauthorized material or transmittal to wrong parties. APHIS uses policy-controlled, tiered approval processes that ensures evaluation of all aspects of the transmittal process to validate the appropriate and legality of such information transfer. Employees are instructed and trained to guard the information about stakeholders, cooperators, etc, from any unauthorized person.

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

Yes

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

Yes

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

Data sharing will depend upon the application. Each circumstance could be different and will be reflected in the program application PIA.

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

Notification will depend upon the application – notification includes privacy banner, MOUs, verbally and in writing.

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?

Any individual may obtain information from a record in the system that pertains to them. Requests for records must follow the guidelines established by the Freedom of Information Act as outlined on the APHIS webpage. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road, Unit 50, Riverdale, MD 20737-1232

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

Each application has a SORN for the records they are collecting and has points of contact to report and correct inaccurate or erroneous information.

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

Contributors may contact the individual points of contact for each system using the GIS Cloud for their applications.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

No privacy risks because redress is done according to guidelines set forth by the Freedom of Information Act Staff.

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?

Role based access controls and personnel security policies will be implemented and followed. All system access is based on a need-to-know basis.

8.2 Will Department contractors have access to the system?

Yes in certain situations

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

All users are required to take annual Department/Agency privacy and Computer Security training.

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

Currently undergoing Accreditation and Authorization testing.

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

Robust authentication and authorization via USDA eAuth, physical access control, firewalls, intrusion detection systems and system auditing are among the countermeasures used to prevent unauthorized access and misuse of data.

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?

All system disclosure will depend upon the application using the GIS Cloud.

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 APHIS GIS Cloud provides the connectivity platform for APHIS programs to use GIS services within a Cloud environment. APHIS uses geographic information system (GIS) in the field and office environments to conduct animal and plant surveys, sampling, monitoring, analysis and reporting. The use of GIS data and analysis has become an integral part of how APHIS conducts businesses.

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

This is a cloud based system, there is some risk that unauthorized intruders could gain access to privacy information. However, the ESRI Cloud system is FedRAMP certified and all security controls are in place according to their certification.

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?

None at this time

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

None at this time

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

N/A

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?

N/A

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

N/A

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

N/A

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?

N/A

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)?

N/A

10.10 Does the system use web measurement and customization technology?

N/A

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

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

N/A

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

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.

N/A

Approving Officials

Patrick J. McFall
Animal and Plant Health Inspection Service
United States Department of Agriculture

Rajiv Sharma
Information System Security Program Manager
Animal and Plant Health Inspection Service
United States Department of Agriculture

Tonya Woods
APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture